



DSB Task Force on

# CYBER SUPPLY CHAIN



THIS PAGE INTENTIONALLY BLANK

REPORT OF THE DEFENSE SCIENCE BOARD

TASK FORCE ON

# Cyber Supply Chain

February 2017



Office of the Under Secretary of Defense  
For Acquisition, Technology, and Logistics  
Washington, D.C. 20301-3140

This report is a product of the Defense Science Board (DSB).

The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense. The Defense Science Board Task Force on Cyber Supply Chain completed its information-gathering in May 2016. The report was cleared for public release on February 6, 2017.

This report is unclassified and cleared for public release.



DEFENSE SCIENCE  
BOARD

OFFICE OF THE SECRETARY OF DEFENSE  
3140 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3140

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION,  
TECHNOLOGY, AND LOGISTICS

SUBJECT: Final Report of the Defense Science Board (DSB) Task Force on Cyber Supply Chain

I am pleased to forward the final report of the DSB Task Force on Cyber Supply Chain. The study proposes recommendations to strengthen the supply chain of microelectronics that are inserted into Department of Defense weapons systems.

Given the dynamic nature of the global market for microelectronics, the Department must operate in a rapidly evolving environment to assure parts in the cyber supply chain. The report recommends expanding cyber supply chain exercises in the Military Services to address warfighter challenges while also improving program protection practices over the lifecycle of weapons systems.

I fully endorse all of the recommendations contained in this report and urge their careful consideration and adoption.

A handwritten signature in black ink, appearing to read "Craig Fields", is positioned above the printed name.

Craig Fields  
Chairman



DEFENSE SCIENCE  
BOARD

OFFICE OF THE SECRETARY OF DEFENSE  
3140 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3140

MEMORANDUM TO THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Final Report of the Defense Science Board Task Force on Cyber Supply Chain

Attached is the final report of the Defense Science Board Task Force on Cyber Supply Chain. The task force assessed the organization, missions, and authorities that encompass the use of microelectronics and components in Department of Defense (DoD) weapons systems. The task force addressed:

- practices to mitigate malicious supply chain risk and latent vulnerabilities, and whether opportunities exist to modify or strengthen these practices;
- current Department program protection processes, as well as other practices to detect and assess potential vulnerabilities in hardware and software;
- the extent to which commercial off the shelf vulnerabilities have been reported and impact the security of DoD systems; and
- interagency activities that DoD could better leverage to reduce supply chain risks.

The task force found that the capital cost of maintaining a DoD-owned Trusted Foundry is not a feasible expense. The task force recommends that the Department develop a long-term strategy for access to state-of-the-art commercial foundry capabilities that does not rely exclusively on trust; and continue research and development (R&D) investments of DoD agencies for a technology-enabled strategy that fosters new tools to better defend against cyber supply chain attacks.

The task force concluded that the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) must strengthen lifecycle protection policies, enterprise implementation support, and R&D programs to ensure that DoD weapons systems are designed, fielded, and sustained in a way that reduces the likelihood and consequences of cyber supply chain attacks.

Hon. Paul "Page" Hoyer  
Co-chair

Dr. John Manferdelli  
Co-chair

## Table of Contents

# Table of Contents

<b>Executive Summary .....</b>	<b>1</b>
<b>Chapter 1: Understanding Supply Chain Risk .....</b>	<b>6</b>
1.1 The Attack Surface: Multiple Sectors, Multiple Supply Chains.....	6
1.2 Types of Malicious Attacks.....	8
1.3 Cyber Vulnerability Assessments.....	9
<b>Chapter 2: Mitigating Potential Vulnerabilities.....</b>	<b>12</b>
2.1 Protecting Supply Chains .....	12
2.2 Detecting and Reporting Attacks on Supply Chains.....	14
2.3 Responding to and Recovering from Attacks.....	18
<b>Chapter 3: Approaching Acquisition Differently .....</b>	<b>20</b>
3.1 Improving Program Protection Plans.....	20
3.2 Supplier Vetting .....	24
3.3 Supporting Program Offices to Improve Assurance .....	27
3.4 Cybersecurity for Commercial and Open Source Components .....	32
<b>Chapter 4: Supporting Lifecycle Operations .....</b>	<b>37</b>
4.1 Program Protection Planning for Fielded Systems .....	37
4.2 Collect and Act on Parts Vulnerabilities.....	40
<b>Chapter 5: Pursuing Technical Solutions.....</b>	<b>44</b>
5.1 Custom Fabrication of State-Of-The-Art Microelectronics.....	44
5.2 Split Fabrication and Other Alternatives .....	45
5.3 Additonal Research.....	47
<b>Chapter 6: Summary.....</b>	<b>48</b>
<b>Appendix A: Directions for Research to Assure Supply Chain Security .....</b>	<b>52</b>
<b>Appendix B: Cyber Awakening Exercises .....</b>	<b>58</b>
<b>Appendix C: Joint Federated Assurance Center Charter.....</b>	<b>59</b>
<b>Terms of Reference.....</b>	<b>65</b>
<b>Members of the Study .....</b>	<b>66</b>
<b>Briefers to the Study.....</b>	<b>67</b>

---

Figures and Tables

## Figures and Tables in the Report

<b>Figure 1:</b> Multiple industry sectors feed three DoD supply chains .....	7
<b>Figure 2:</b> An attacker seeks opportunities to perform a malicious insertion.....	8
<b>Figure 3:</b> An attacker can bypass the need for malicious insertion by exploiting existing latent vulnerabilities.....	9
<b>Figure 4:</b> Blue approaches can mitigate supply chain exploitation.....	12
<b>Figure 5:</b> Recommended JAPEC and JFAC roles to enhance shared supply chain situational awareness .....	31
<b>Figure 6:</b> Program protection activities can inform solicitations.....	38
<b>Table 1:</b> System Criteria to Detect Counterfeit Electronic Parts .....	16
<b>Table 2:</b> Summary of Recommendations.....	49



## Abbreviations and Acronyms

# Acronyms and Abbreviations

ACQ: acquisition management

AIS: Automated Indicator Sharing

AMRAAM: Advanced Medium-Range Air-to-Air Missile

AMRDEC: Army Aviation and Missile Research, Development, and Engineering Center

ASA(ALT): Assistant Secretary of the Army (Acquisition, Logistics and Technology)

ASDB: Acquisition Security Data Base

ASD(C3I): Assistant Secretary of Defense for Command, Control, Communications and Intelligence

ASD(L&MR): Assistant Secretary of Defense for Logistics and Materiel Readiness

ASD(R&E): Assistant Secretary of Defense for Research and Engineering

ASICs: application specific integrated circuits

ASLR: address space layout randomization

BIOS: basic input and output system

BSIMM: Building Security in Maturity Model

C4ISR: command, control, communications, computers, intelligence, surveillance and reconnaissance

CAD: computer-aided design

CERT: Computer Emergency Readiness Team

CII: Core Infrastructure Initiative

CIO: chief information officer

CISA: Cybersecurity Information Sharing Act

CJCS: Chairman of the Joint Chiefs of Staff

CMOS: complementary metal-oxide-semiconductor

CMU SEI: Carnegie Mellon University Software Engineering Institute

## **Abbreviations and Acronyms**

CND: computer network defense

COTS: commercial off the shelf

CPI: critical program information

CTI: controlled technical information

DARPA: Defense Advanced Research Projects Agency

DASD(Research): Deputy Assistant Secretary of Defense for Research

DASD(SE): Deputy Assistant Secretary of Defense for Systems Engineering

DAU: Defense Acquisition University

DC3: DoD Cyber Crime Center

DCS: distributed control systems

DIA: Defense Intelligence Agency

DIB: defense industrial base

DIBNet: Defense Industrial Base Network

DFARS: Defense Federal Acquisition Regulation Supplement

DHS: Department of Homeland Security

DISA: Defense Information Systems Agency

DIUx: Defense Innovation Unit Experimental

DLA: Defense Logistics Agency

DMEA: Defense Microelectronics Activity

DoD: Department of Defense

DoDI: Department of Defense Instruction

DRAM: dynamic random access memory

DSB: Defense Science Board

fab: semiconductor fabrication plant

FAR: Federal Acquisition Regulation

## **Abbreviations and Acronyms**

FIPS: Federal Information Processing Standard

FPGA: field programmable gate array

GCHQ: Government Communications Headquarters

GIDEP: Government-Industry Data Exchange Program

GSA: General Services Administration

IA: information assurance

IARPA: Intelligence Advanced Research Projects Activity

IAVA: Information Assurance Vulnerability Alert

IBM: International Business Machines

ICS-CERT: Industrial Control Systems Cyber Emergency Response Team

IEC: International Electrotechnical Commission

IOC: initial operational capability

ISAC: Information Sharing and Analysis Center

ISAO: Information Sharing and Analysis Organization

ISO: International Organization for Standardization

JAPEC: Joint Acquisition Protection and Exploitation Cell

JFAC: Joint Federated Assurance Center

LCSP: Life Cycle Sustainment Plan

MDA: Missile Defense Agency

MORE: Multifunctional Obsolescence Resolution Environment

NCCIC: National Cybersecurity and Communications Integration Center

NDAA: National Defense Authorization Act

NIAP: National Information Assurance Partnership

NIST: National Institute of Standards and Technology

NRO: National Reconnaissance Office

## **Abbreviations and Acronyms**

NSA: National Security Agency

ODNI: Office of the Director of National Intelligence

OEM: original equipment manufacturer

OGC: Office of General Counsel

OSS: open source software

O-TTPS: Open Trusted Technology Provider™ Standard

PEO: Program Executive Office

PM: program manager

PO: program office

PPP: Program Protection Plan

PUF: physically unclonable function

R&D: research and development

RDT&E: research, development, test, and evaluation

SAE: Service Acquisition Executive

SAF/AQX: Secretary of the Air Force for Acquisition Integration

SAFECode: Software Assurance Forum for Excellence in Code

SCADA: Supervisory Control and Data Acquisition

SGX: Software Guard Extensions

SP: Special Publication

TPM: Trusted Platform Module

TTRA: technology targeting risk assessment

USB: universal serial bus

US-CERT: United States Computer Emergency Readiness Team

USD(AT&L): Under Secretary of Defense for Acquisition, Technology and Logistics

USD(I): Under Secretary of Defense for Intelligence

## Executive Summary

# Executive Summary

Modern weapons systems have depended on microelectronics since the inception of integrated circuits over fifty years ago. Today, most electronics contain programmable components of ever increasing complexity.<sup>1, 2</sup> At the same time, the Department of Defense (DoD) has become a far less influential buyer in a vast, globalized supplier base.<sup>3</sup> Consequently, assuring that defense electronics are free from vulnerabilities is a daunting task.<sup>4</sup>

Because system configurations typically remain unchanged for very long periods of time, compromising microelectronics can create persistent vulnerabilities. Exploitation of vulnerabilities in microelectronics and embedded software can cause mission failure in modern weapons systems. Such exploitations are especially pernicious because they can be difficult to distinguish from electrical or mechanical failures and because effects can run the gamut from system degradation to system failure to system subversion.

Cyber supply chain vulnerabilities may be inserted or discovered throughout the lifecycle of a system. Of particular concern are the weapons the nation depends upon today; almost all were developed, acquired, and fielded without formal protection plans.

## MALICIOUS INSERTION AND THE EXPLOITATION OF LATENT VULNERABILITIES

Insertion of a malicious microelectronic vulnerability via the supply chain can occur at any time during production and fielding of a weapons system or during sustainment of the fielded system. No matter where an attack occurs in the lifecycle of the system, an attacker seeking to exploit a maliciously inserted vulnerability must execute each step in the kill chain:

- **Intelligence and planning:** gathering information on target system and suppliers to develop supply chain attack vector.
- **Design and create:** developing malicious hardware or software for insertion into target supply chain. May be done in an attacker-owned facility or by an insider in a legitimate facility.
- **Insert:** incorporating malicious hardware or software into target system through its supply chain.
- **Achieve effect:** actuating and operating malicious hardware or software to achieve an effect.

---

1. For example, the BA 5590 battery, used in numerous systems, incorporates a “smart” state-of-charge indicator.  
2. Basic input and output system (BIOS) complexity increased by a factor of  $10^6$  between 1999 and 2015.  
3. DoD now buys less than one percent of application specific integrated circuits (ASICs), and an even smaller percentage of commodity electronics.  
4. See Appendix A for a discussion of fundamental approaches to assurance.

## Executive Summary

While there has been some emphasis on denying the attacker information about the target system and suppliers, DoD has focused primarily on denying malicious insertion through use of “trusted” sources, where trust is determined by the pedigree of the supplier.

The task force observed instances that may have been unsuccessful attacks on critical weapons systems via malicious insertion. It is difficult to know whether such activity is widespread, but the existence of counterfeit electronics in the supply chain demonstrates the potential for such attacks.<sup>5</sup> When done effectively, malicious insertion will not be detectable until actuated and it may present as a design flaw when ultimately observed.

Exploitation via malicious insertion has, however, been confirmed in the commercial sector. Prominent recent examples include Volkswagen’s insertion of a “defeat device” to thwart emissions testing and insertion of embedded code into Juniper® routers.<sup>6, 7</sup> Recently, FTDI, a semiconductor device company, used a Windows driver update to completely disable computers using functional clones of some component chips, demonstrating the full cycle of component insertion, subsequent activation, and effect.<sup>8</sup>

Complex microelectronics will inevitably contain latent vulnerabilities. Diligent test protocols, while an essential best practice, cannot guarantee that systems will be free of such vulnerabilities.<sup>9</sup> Vulnerabilities in widely distributed commercial microelectronics have been discovered years after these components were sold into the market.<sup>10</sup> Even where no single major vulnerability exists, attacks may exploit a series of subtle design issues that may be widely distributed.<sup>11</sup> If an attacker can gain access to weapons system design information and discover a useful latent vulnerability, it is possible to bypass the costly and potentially risky process of malicious insertion.

- 
5. Department of Commerce, *Defense Industrial Base Assessment: Counterfeit Electronics*, [January 2010]. Available at: [https://www.bis.doc.gov/index.php/forms-documents/doc\\_view/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010](https://www.bis.doc.gov/index.php/forms-documents/doc_view/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010) (Accessed September 2016.)
  6. Russell Hotten, “Volkswagen: The scandal explained.” *BBC News* [December 10, 2015]. Available at: [www.bbc.com/news/business-34324772](http://www.bbc.com/news/business-34324772) (Accessed October 2016.)
  7. Brad Duncan, October 28, 2016 (12:51 p.m.), “ScreenOS vulnerability affects Juniper firewalls,” InfoSec Handlers Diary Blog, [December 18, 2015]. Available at: <https://isc.sans.edu/diary/ScreenOS+vulnerability+affects+Juniper+firewalls/20511> (Accessed October 2016.)
  8. James Sanders, “FTDI abuses Windows Update, pushing driver that breaks counterfeit chips,” *TechRepublic* [February 2, 2016]. Available at: <http://www.techrepublic.com/article/ftdi-abuses-windows-update-pushing-driver-that-breaks-counterfeit-chips> (Accessed September 2016.)
  9. This is true for all but the simplest systems.
  10. For example, dynamic random-access memory (DRAM) modules susceptible to the Rowhammer effect were produced beginning in 2010. The vulnerability of these DRAMs to attack leading to privilege escalation was published in 2015. Essentially all computers manufactured during this period had this vulnerability. See *Google Project Zero* blog, available at: <https://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html> (Accessed December 2016.)
  11. Andy Greenberg, “Wickedly Clever USB Stick Installs a Backdoor on Locked PCs,” *Wired Magazine*, [November 16, 2016]. Available at: [www.wired.com/2016/11/wickedly-clever-usb-stick-installs-backdoor-locked-pcs/?mbid=social\\_gplus](http://www.wired.com/2016/11/wickedly-clever-usb-stick-installs-backdoor-locked-pcs/?mbid=social_gplus) (Accessed December 2016.)

## Executive Summary

The extended lifecycles of defense systems increase the probability that an attacker will both gain system knowledge and also discover latent vulnerabilities. Recent exercises by all three Military Services have demonstrated the feasibility and efficacy of exploitation via this shortcut to achieve the desired effect.

### OVERVIEW OF THE CYBER SUPPLY CHAIN LANDSCAPE

The supply chain for microelectronics parts is complex, involving multiple industry sectors. Each sector sells to each of the others. Furthermore, parts may be returned to manufacturers or distributors and subsequently reenter the supply chain making both pedigree and provenance difficult to track using current procedures. This complex of industry segments feeds three supply chains: the DoD acquisition supply chain, the DoD sustainment supply chain, and the global commercial supply chain. Each supply chain is subject to attack and each offers differing costs and benefits to an attacker.

In 2011, recognizing the DoD's heavy reliance on integrated circuits produced outside the United States to achieve cutting edge technology, the Undersecretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) instructed program managers (PMs) to address supply chain threats in their Program Protection Plans (PPPs). PPPs are intended to take a comprehensive approach in considering all aspects of system security, including cybersecurity, and address initial steps to safeguard unclassified program information.

Programs subject to milestone decisions are required to conduct program protection activities and document the results in PPPs for approval by the Milestone Decision Authority at each acquisition milestone. Review of the program protection processes across the Department shows that security and information system managers address security primarily after the system design has been completed.

Current PPPs, however, do not carry over robustly to the sustainment phase. There is little evidence that robust program protection activities continue after a system has been fielded or that documentation is being maintained as the system continues to evolve through sustainment. By the time a defense system is fielded, microelectronic components in that system are likely to be obsolete and may be unavailable from the original equipment manufacturer (OEM) or its sub-tier suppliers. This may force DoD to purchase from distributors where pedigree is less secure and provenance is more difficult to track. Furthermore, the longer a system is in the field with the same microelectronic parts and embedded software, the more likely it is that adversaries will be able to gain system information and to insert or discover vulnerabilities. As these vulnerabilities have been revealed, it has become clear that malicious insertion and discovery of exploitable latent vulnerabilities are concerns in both the acquisition and sustainment supply chains.

Active search and automated monitoring can expose vulnerabilities. Cyber Awakening exercises have discovered exploitable cyber supply chain vulnerabilities in key weapons systems. The results of such exercises, if conducted regularly on major weapons systems and subsystems, would be highly relevant for systems currently in both acquisition and sustainment. There is not yet a mechanism for routinely providing cyber awareness results to Program Executive Offices (PEOs) and program

## Executive Summary

managers, or cyber awareness training to logisticians and hands-on maintenance personnel at appropriate classification levels.

Program management offices are responsible for creating Program Protection Plans. Currently, guidance, expertise, and support for this effort are insufficient, with limited engagement by the system engineering community and limited influence on system design. Program protection planning activities are uneven in quality and focus as some programs focus on protecting microelectronics availability whereas others emphasize protection of personnel or system security. The task force believes that the proper focus should be on reducing the probability of mission failure. The Joint Federated Assurance Center (JFAC) should be used as a much needed source of expertise in support of program managers to assist with life cycle program protection planning and system security engineering.

In typically long DoD acquisition processes, approximately 70 percent of electronics in a weapons system are obsolete or no longer in production prior to system fielding.<sup>12</sup> The Department's mechanisms for tracking inventory obsolescence and vulnerabilities in microelectronic parts are inadequate. Microelectronics components are likely to become obsolete repeatedly during the weapons system lifecycle. Efforts to track component obsolescence lack oversight at a Department-wide level.<sup>13</sup> Reporting of counterfeit and "suspect-counterfeit" microelectronics is mandatory for some, but not all prime contracts and subcontracts. Such reporting requirements are inconsistent and no DoD system at present collects event information on cyber-physical attacks of electronic components as its primary function. To address these concerns, a shared vulnerability database and a parts application database of installed hardware could promulgate corrective actions across weapons systems.

DoD will have a continuing need for access to trustworthy, state-of-the-art, application specific integrated circuits (ASICs). That need is likely to grow for systems that support intelligent or autonomous capabilities. The current Trusted Foundry program provides an interim solution through the leveraging of a dual-use commercial facility, but foreign ownership and global commercial competition will reduce DoD's ability to impose restrictions on the workforce.

The Department will need to analyze this risk and define a long-term strategy that includes plans for design, fabrication, and logistics. The design phase needs to be protected from both malicious manipulation and design exfiltration, but trusted ASIC design is within DoD's ability to control at a low level of risk. Promising research results from the Defense Advanced Research Projects Agency (DARPA), the Intelligence Advanced Research Projects Activity (IARPA), and other agencies offer the potential for a technology-enabled strategy that can use widely sourced parts confidently rather than depending on a sole source Trusted Foundry. Continued research and development (R&D) is needed, and a framework is provided in Appendix A that can serve as a basis for planning further R&D investment programs.

---

12. U.S. Army Aviation and Missile Research, Development, and Engineering Center (AMRDEC), "Success Stories – The MORE Tool." Available at: <https://www.amrdec.army.mil/amrdec/success-more.html> (Accessed November 2016.)

13. U.S. Government Accountability Office, *Counterfeit Parts: DoD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk*, GAO-16-236 [2016]. Available at: <http://www.gao.gov/products/GAO-16-236> (Accessed December 2016.)



## **Executive Summary**

Weapons in the field today are of special concern. They were not developed under the Program Protection Plans in place today. Also, critical components were not identified in a consistent manner and original suppliers were not subject to the vetting now required. Any existing vulnerabilities continue with no formal process for mitigation.

### **OVERARCHING RECOMMENDATIONS**

The task force recommends that USD(AT&L) strengthen lifecycle protection policies, enterprise implementation support, and R&D programs. Such efforts will ensure that systems are designed, fielded, and sustained in a way that reduces the likelihood and consequence of cyber supply chain attacks.

In addition, the task force recommends that USD(AT&L) direct development of sustainment Program Protection Plans for critical fielded weapons systems. Military Service Chiefs should designate fielded weapons systems for development of initial sustainment PPPs to demonstrate their effectiveness.

### **SUMMARY**

The nation's weapons systems are at risk from the malicious insertion of defects or malware into microelectronics and embedded software, and from the exploitation of latent vulnerabilities in these systems. Active search for vulnerabilities using Cyber Awakening exercises can identify and classify vulnerabilities, can enable sharing of vulnerability information, and can inform training needs. Most importantly, the effective use of expert resources will improve protection against cyber threats throughout a weapons systems lifecycle.

# Chapter 1: Understanding Supply Chain Risk

In November 2014, the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) directed the Defense Science Board (DSB) to form a task force on Cyber Supply Chain to review the Department's supply chain risk management activities that mitigate the potential for insertion of defects and malware into components that eventually find their way into defense systems. DoD is increasingly reliant on a global supply chain with multiple opportunities for an adversary to taint components or otherwise exploit hardware vulnerabilities. The DSB task force studied the supply chains that provide microelectronic hardware and embedded software aimed at identifying needs and opportunities for the Department to identify, protect, detect, respond to, and recover from attacks involving malicious insertion and exploitation of latent vulnerabilities across the lifecycle of weapons systems.

## 1.1 THE ATTACK SURFACE: MULTIPLE SECTORS, MULTIPLE SUPPLY CHAINS

The defense microelectronics supply chain is not a simple linear hierarchy of suppliers, but rather a complex web of interactions among original component manufacturers (mostly commercial), authorized and independent distributors and brokers, circuit board assemblers, defense prime contractors and subcontractors, and defense sustainment activities such as supply agencies and maintenance depots. Buyer-seller relationships in this environment are fluid. Visibility to the lowest level of supply is obscured by proprietary business transactions at each level, making assurance to the lowest tier supplier possible only by exceptional government procedures that may be unacceptable to commercial suppliers.

When targeting the microelectronics supply chain for a weapons system, an attacker will consider:

- **Access:** can the attacker create opportunities, or leverage existing opportunities, to place malicious hardware or software into the weapons system?
- **Precision Effects:** to what extent can the malicious insertion be relied upon to affect the weapons system's performance, preferably in a predictable and controllable way?

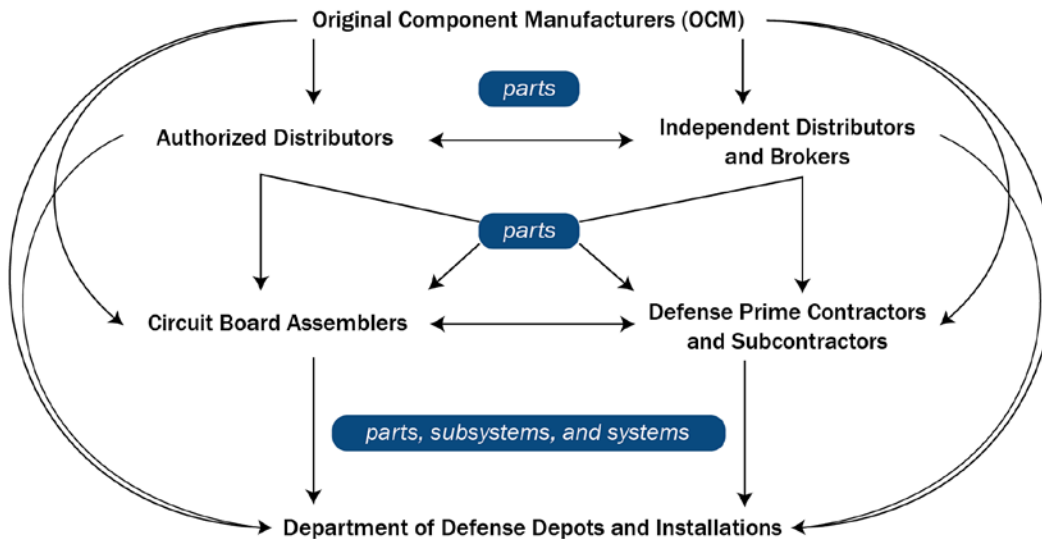
Figure 1 depicts the web of suppliers that support three interconnected DoD supply chains.<sup>14</sup> Understanding these three supply chains will help characterize the susceptibility of each system's supply chain to attacks:

1. **The global commercial supply chain:** This is the source of most microelectronic components. It feeds the other two supply chains and is the most accessible for malicious insertion. As a result of the complex interactions between suppliers, and because defense is a small fraction of the total market, it is difficult to predict which specific parts of this supply chain will ultimately be placed

---

14. Department of Commerce, *Defense Industrial Base Assessment: Counterfeit Electronics*, pg. 4 [January 2010]. Available at: [https://www.bis.doc.gov/index.php/forms-documents/doc\\_view/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010](https://www.bis.doc.gov/index.php/forms-documents/doc_view/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010) (Accessed September 2016.)

## Understanding Supply Chain Risk



**Figure 1:** Multiple industry sectors feed three DoD supply chains.

into a weapons system. This lack of predictability can make it difficult to achieve precision effects on weapons systems through malicious insertions into the global commercial supply chain.

2. **The DoD acquisition supply chain:** This is the supply chain carefully designed by the prime contractor to support weapons-system development and production. It is difficult for an attacker to gain access to this supply chain for malicious insertion. However, if access can be attained, the attacker will have good knowledge of the part's placement in the weapons system, thus leading to a successful attack that can create precise and impactful effects.
3. **The DoD sustainment supply chain:** This supply chain evolves during the weapons system's lifecycle to include competitively selected aftermarket suppliers who are often different from the participants in the acquisition supply chain, and subject to less programmatic oversight. Microelectronic parts obsolescence is a major factor in driving toward new sources of supply for replacement parts. The continued discovery of counterfeit parts in the DoD supply system is proof that criminal activity (with less sophistication than a nation-state adversary) can succeed in penetrating supply chains. Parts provenance in sustainment is harder to track than in acquisition, and there are opportunities for an attacker to gain access. Furthermore, if the attacker has very good knowledge of a part's placement in a weapons system, a successful malicious insertion attack can create precise and impactful results. Therefore, the DoD sustainment supply chain is the most attractive target for sophisticated adversaries who desire to achieve both access and precision effects.

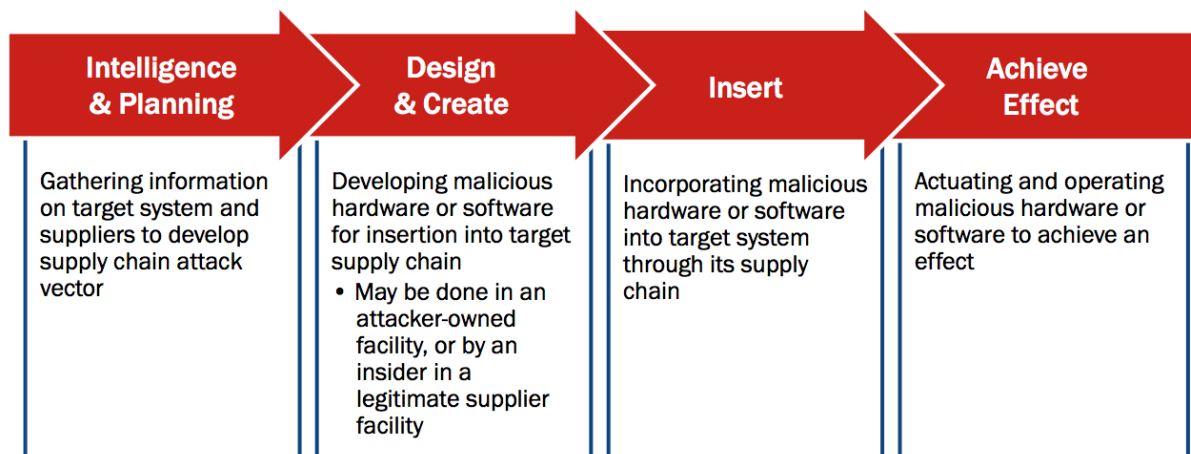
## Understanding Supply Chain Risk

### 1.2 TYPES OF MALICIOUS ATTACKS

Supply chain attacks arise from two principal causes: 1) malicious insertion of defect or malware or 2) exploitation of latent vulnerabilities.

Parts may be deliberately subverted at design time, during fabrication, during transport, or while actually operating in a system via malicious insertion. This is a multi-step process, as shown in Figure 2. The attacker must first gather detailed information on the target system and its suppliers to identify opportunities for access and means to achieve effects through the insertion. With this knowledge, the attacker creates malicious hardware or software (or both) and performs the insertion. Finally, the malicious insertion operates to achieve the attacker's desired effect, possibly actuated by an event or signal. Execution of this full, four-step process for malicious insertion requires significant effort by the attacker, may take years to execute, and requires persistence and patience to achieve the desired effects. While evidence of successful malicious insertion of parts in DoD weapons systems is scarce, recent cases from the commercial sector are sobering reminders that these attacks are possible and can create undesirable effects.<sup>15, 16</sup>

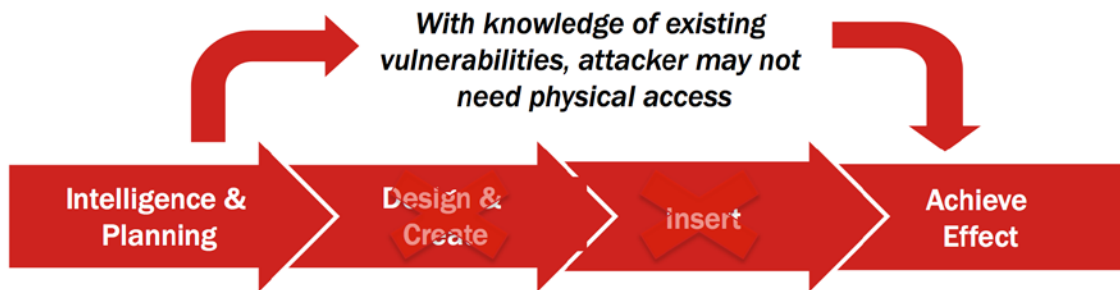
Second, and far more common, parts may have latent vulnerabilities that cause them to function improperly under circumstances that were not foreseen and under conditions that were not tested when the system was first deployed. In this case, the attacker is provided a shortcut that can bypass the need for malicious insertion, as illustrated in Figure 3. Such vulnerabilities are routinely discovered and reported in widely available information sources. Patches, in the form of firmware updates or hardware



**Figure 2:** An attacker seeks opportunities to perform a malicious insertion.

15. Russell Hotten, "Volkswagen: The scandal explained." *BBC News* [December 10, 2015]. Available at: [www.bbc.com/news/business-34324772](http://www.bbc.com/news/business-34324772) (Accessed October 2016.)
16. Brad Duncan, October 28, 2016 (12:51 p.m.), "ScreenOS vulnerability affects Juniper firewalls," *InfoSec Handlers Diary Blog*, [December 18, 2015]. Available at: <https://isc.sans.edu/diary/ScreenOS+vulnerability+affects+Juniper+firewalls/20511> (Accessed October 2016.)

---

**Understanding Supply Chain Risk**

---

**Figure 3:** An attacker can bypass the need for malicious insertion by exploiting existing latent vulnerabilities.

replacements, are often incompletely implemented.

Systems fielded today are particularly susceptible to the second type of attack. The task force estimates that fielded systems make up as much as 80 percent of military capability through 2025. These systems are “static targets” that are in the field for many years. It is often easy for the adversary to know which parts are in which systems because these mappings for repair or replacement are made public in sustainment solicitations. Further targeting information is available to an adversary who has access to design data exfiltrated prior, during, or after the acquisition phase. The desire of adversaries to exfiltrate design data of key weapons systems is a concern because it would offer them a big advantage in targeting for effect based on known parts vulnerabilities, without the need for malicious insertion. The most cost effective and least risky path for an adversary to attack a weapons system may be to exploit existing vulnerabilities and bypass the need for malicious insertion.

### 1.3 CYBER VULNERABILITY ASSESSMENTS

Cyber vulnerabilities can arise from a wide array of causes. A failure might be triggered, for example, by an electromagnetic wave for a particular duration (or in a pattern of emission); a combination of sensor based environmental conditions that may include location, time, temperature, vibration, acoustic signaling (audible or not); patterns of responses from connected systems, or by physically connected cyber devices. Some of these failure modes may be controlled by an adversary and activated in a precise and disastrous manner without warning. The circumstances that may actuate a maliciously modified part or an innocently vulnerable part are so varied and complex that they can never be exhaustively listed or tested.

For this reason, supply chain security benefits from operational measures that deny access to information about identified systems throughout their lifecycle. Unfortunately, access to information on common parts, or even specific long-lived systems, is not easy to conceal for long periods of time, and such concealment measures increase cost and reduce the Department’s ability to rapidly field weapons systems. In addition, the benefit of using parts that are regularly analyzed by a knowledgeable external community of cybersecurity experts may more than balance the benefit from limiting knowledge. Limiting knowledge may also reduce the availability of trained experts and processes to replace or

---

**Understanding Supply Chain Risk**

modify parts and systems determined to be faulty or vulnerable. An additional complication is that many innovations are first conceived and relentlessly improved outside of DoD-controlled facilities, and duplicating such innovations or the underlying technology may be prohibitively expensive and time consuming.

Large, technically sophisticated, even relatively cost-insensitive commercial entities also confront cyber supply chain issues for similar reasons. Cyber-active systems (such as automobiles) have been remotely and successfully attacked by small groups of researchers expending modest resources over a very short period.<sup>17</sup>

Another example involving commercial-malicious physical insertion is the Volkswagen emissions scandal. In this case, the vehicle manufacturer undermined emissions testing by installing firmware to cause the vehicle to operate in a clean emissions mode during testing, but to operate in a more efficient mode with much higher emissions during regular operations. This example, which raised a more modest concern about physical safety, demonstrates the feasibility, extent, and difficulty of detection of attacks on cyber-supply chains.<sup>18</sup>

In the face of all these challenges, the Department must ensure the proper operation of its existing and future weapons systems. Many of these systems were designed and manufactured before DoD had the opportunity to carry out potential supply chain protection activities such as:

1. Careful engineering design beginning at system inception to prevent failure based on complex environmental cues;
2. Carefully planned manufacturing practices to prevent the introduction or malicious insertion of vulnerabilities;
3. Diligent protection from tampering of parts during design, shipment, and operation;
4. Active search and continuous automated monitoring to detect system failure;
5. Resilient design that allows for rapid isolation of subsystems based on detected aberrant behavior and rapid part substitution or replacement of or updating of software components of the subsystem in whole or in part; and
6. Practiced, efficient response procedures at the subsystem, system and mission level to enable remediation in response to detected or anticipated failure, as well as emerging information on new vulnerabilities and exploits.

In the absence of addressing all of these protection measures, there are several important examples in which the Military Services have employed Cyber Awakening exercises to test vulnerability to supply

---

17. Andy Greenberg, "The FBI Warns that Car Hacking is a Big Risk," *Wired Magazine*, [March 17, 2016]. Available at: <https://www.wired.com/2016/03/fbi-warns-car-hacking-real-risk> (Accessed October 2016.)

18. Russell Hotten, "Volkswagen: The scandal explained." *BBC News* [December 10, 2015]. Available at: [www.bbc.com/news/business-34324772](http://www.bbc.com/news/business-34324772) (Accessed October 2016.)

---

## Understanding Supply Chain Risk

chain attacks.<sup>19</sup> These exercises offer valuable insight into the ability of each Military Service to identify the extent to which an attack may be effective.

The task force recommends that each Military Service Chief conduct at least one full-system cyber exercise, including practical full-system staged attacks to assess the extent of a system's vulnerability. These assessments are not a substitute for comprehensive appraisals of each critical system throughout their lifetime. Rather, this measure is an immediate and cost effective mechanism to build capacity and identify crosscutting problems. In addition, Cyber Awakening assessments offer the following benefits:

1. They identify vulnerabilities in components used in weapons systems. Once weaknesses are identified, these systems can be "hardened" against attacks in a practical and cost effective way.
2. These assessments can point to monitoring activities that would identify some attacks as they are happening. Identification of attacks can allow system reconfiguration and mission adjustments that block the attack while a mission is underway.
3. The assessments help identify material that can be used to train operators and system maintainers, who can implement procedural changes.
4. Knowledge of these vulnerabilities enables DoD to develop acquisition guidance preventing many of these attacks in new and replacement systems.
5. Commanders will be provided with the situational awareness to enable mission planners and commanders to recognize the danger presented potential attacks prior to missions and to develop plans and procedures to "fight through" attacks as they occur.

The principal advantage in conducting at least one exercise per Military Service is that the subsequent assessments will foster actionable activities that offer the "biggest bang for the buck" in making effective improvements for existing systems in a time of tight budgets. Such activities will impose cost on the adversary as well as increase the risk for an adversary to target DoD systems.

### RECOMMENDATION 1

**Military Service Chiefs, with Military Deputies of the Service Acquisition Executives (SAEs),** conduct at least one Cyber Awakening exercise per year and use the results of these assessments, in timely training of acquisition, operational, and sustainment personnel:

- The training should be frequently updated as new exercises are conducted.
- In-person training should be provided at the appropriate classification level for all affected personnel.

---

19. See Appendix B for more information on the DoD's Cyber Awakening exercises.

## Chapter 2: Mitigating Potential Vulnerabilities

Many of the procedures that have been developed and implemented to mitigate vulnerabilities in networks and software systems also apply to hardware vulnerabilities. At the highest level, these procedures are to *protect* critical information and systems, *detect* an attack when it occurs, *respond* (i.e., fight through the attack), and *recover* (i.e., restore the system to a trusted state), as shown in Figure 4.

When examining the areas mitigating supply chain attacks in current DoD practices, *Protect* is better addressed via the PPP process, although more attention on resilience and agility in design is needed. *Detect* is both a system design and training issue that needs more emphasis, and *Respond and Recover* are operational issues that need more attention from the Military Services.

### 2.1 PROTECTING SUPPLY CHAINS

Supply chain vulnerability can be reduced by protecting design and supplier information; protecting design, manufacturing, and distribution systems; and employing better assurance of parts provenance. In addition, design strategies that provide built-in active monitoring improve the ability to detect exploitation and respond.<sup>20</sup> Modular system architectures that isolate functions and provide fail-over capabilities can improve the ability to respond and fight through an attack. System architectures that provide for rapid upgrades can improve the ability to recover from an attack by eliminating the affected components.

DoD policies and practices currently emphasize *Protect* activities more than *Detect*, *Respond*, or *Recover* activities. Today, the primary method to protect DoD systems is through program protection planning and documenting the results in Program Protection Plans (PPPs). Each acquisition program is required to address program protection planning and present a PPP at acquisition milestones. According to Department of Defense Instruction (DoDI) 5000.02, program protection planning is “the integrating process for managing risks to DoD warfighting capability from foreign intelligence collection; from hardware, software, and cyber vulnerability or supply chain exploitation; and from battlefield loss throughout the system lifecycle.”

The PPP is a single source document used to coordinate and integrate all protection efforts for a



**Figure 4:** Blue approaches can mitigate supply chain exploitation.

20. The design authority must be careful not to expand the attack surface by including such monitoring.



---

**Mitigating Potential Vulnerabilities**

defense acquisition program. Each PPP is intended to:

*Identify the program's critical program information and mission-critical functions and components; the threats to and vulnerabilities of these items; the plan to apply countermeasures to mitigate associated risks; and planning for exportability and potential foreign involvement. Countermeasures should include anti-tamper, exportability features, security (including cybersecurity, operations security, information security, personnel security, and physical security), secure system design, supply chain risk management, software assurance, anti-counterfeit practices, procurement strategies, and other mitigations ... Countermeasures should mitigate or remediate vulnerabilities throughout the product lifecycle, including design, development, developmental and operational testing, operations, sustainment, and disposal.<sup>21</sup>*

Each PPP defines what is critical, in terms of information and functionality to be protected, with substantial variability across programs. Programs have a natural desire to keep the “critical” list as short as possible. The specialized skills needed to identify and mitigate hardware and software vulnerabilities are unlikely to exist in program office staffs, and must be sourced externally. Design for security and resilience may compete with cost, schedule, and performance pressures. Mechanisms for assessing the program level impacts of threats identified by the intelligence community are not widely employed in program offices. Mitigation of supply chain risks is difficult, and the standard PPP process is to rely primarily on Defense Intelligence Agency (DIA) vetting of critical suppliers—a “point in time” solution at best.

Sharing threat, vulnerability, and mitigation information across program PPPs is not well supported in current practice. While the PPP fits well into the program-by-program oversight process in defense acquisition, it does not benefit the enterprise-wide dimension to the problem. One Congressionally-mandated organization to offer the possibility of supporting programs with enterprise-informed expertise in program protection is the Joint Federated Assurance Center (JFAC).<sup>22</sup> An additional organization to offer the possibility of supporting programs with enterprise-wide coordinated threat analyses is the Joint Acquisition Protection and Exploitation Cell (JAPEC), which was directed by the Secretary of Defense in 2013<sup>23</sup>:

- The Joint Federated Assurance Center (JFAC) is chartered to develop, maintain, and offer software and hardware vulnerability detection, analysis, and remediation capabilities through a federation of internal, coordinated organizations and facilities from across the Military Departments, Defense Agencies, and other DoD organizations.<sup>24</sup>
- The Joint Acquisition Protection and Exploitation Cell (JAPEC) integrates and coordinates analysis to enable controlled technical information (CTI) protection efforts across the DoD

---

21. USD(AT&L), *Operation of the Defense Acquisition System*, DoD Instruction (DoDI) 5000.02, [January 7, 2015], Enclosure 3, pg. 86.

22. *National Defense Authorization Act (NDAA) for Fiscal Year 2014*, Public Law 113–66 {December 2013}, Section 937.

23. Secretary of Defense Memorandum, *Safeguarding Unclassified Controlled Technical Information*, October 10, 2013.

24. See Appendix C for JFAC charter.

---

## Mitigating Potential Vulnerabilities

enterprise to proactively mitigate future losses, and exploit opportunities to deter, deny, and disrupt adversaries that may threaten U.S. military advantage. DoD will conduct comprehensive risk and damage assessments of cyber espionage and theft to inform requirements, acquisition, programmatic, and counterintelligence courses of action.<sup>25</sup>

At the end of FY16, USD(AT&L) has approved 76 Acquisition Category 1D/1AM programs since PPP content was formally expanded beyond anti-tamper protection in July 2011.<sup>26</sup> However, many fielded systems do not have a PPP that contains this expanded content because they were fielded prior to 2011, before this requirement was put in place. Handoff of the PPP from the acquisition program manager to lifecycle program manager is embryonic, but recent additions to the “Cybersecurity in Defense Acquisition System” policy emphasize the need to transition the PPP, protect fielded systems, and update threat and vulnerability assessments through the life of the system.<sup>27</sup>

## 2.2 DETECTING AND REPORTING ATTACKS ON SUPPLY CHAINS

Current practices in the *Detect* area of supply chain exploitation are less well developed than the program protection activities. Needs in this area are primarily in the operations and support phase of the lifecycle—after acquisition—although they are addressed initially in the PPP and in system design. For example, during operations and support phase, the supply chain changes and vulnerabilities and new exploit techniques are discovered, but there is little or no capability to detect or track these by weapons system. Parts obsolescence may limit replacement sources to a few non-traditional suppliers, increasing the chance of buying vulnerable or maliciously modified parts. Beyond the test and evaluation phase of acquisition, there is typically no routine training for operators or maintenance crews to detect anomalies that may indicate vulnerabilities have been exploited.

Cyber supply chain threats extend to the software, firmware, and hardware of electronic systems utilized in defense systems. At present, DoD regulations direct the detection of electronic parts that are suspect or confirmed as “counterfeit electronic parts.”<sup>28</sup> The Defense Federal Acquisition Regulation Supplement (DFARS) was recently revised to exclude “embedded software or firmware” from the definition of “counterfeit electronic part.”<sup>29</sup> As a result, DFARS does not presently require that DoD

---

25. Department of Defense, *2015 DoD Cyber Strategy*. Available at: [http://www.defense.gov/Portals/1/features/2015/0415\\_cyber-strategy/Final\\_2015\\_DoD\\_CYBER\\_STRATEGY\\_for\\_web.pdf](http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf) (Accessed November 2016.)

26. See acquisition category information at: <https://dap.dau.mil/glossary/pages/1382.aspx> (Accessed December 2016.)

27. USD(AT&L), *Cybersecurity in the Defense Acquisition System*, DoD Instruction 5000.02, [January 26, 2017], Enclosure 14, pg. 170.

28. Code of Federal Regulations, “Contractor Counterfeit Electronic Part Detection and Avoidance System,” Title 48, 252.246-7007.

29. See Proposed Rule, “Detection and Avoidance of Counterfeit Electronic Parts – Further Implementation,” Sep. 21, 2015, 80 Fed. Reg. 56939, 56941, Final Rule, “Detection and Avoidance of Counterfeit Electronic Parts – Further Implementation,” Aug. 2, 2016, 81 Fed. Reg. 50635, 50649. As explained in the September 2015 Proposed Rule: “Although electronic parts may include embedded software or firmware, the requirements of this rule are more applicable to hardware. Further industry standards are still under development to address testing of embedded software or firmware in electronic parts.”

---

**Mitigating Potential Vulnerabilities**

contractors act to detect or avoid electronic parts that may suffer from malware in embedded software or firmware. While the DFARS has utility to respond to the “physical” threat that a counterfeit part may not perform as an authentic part would, this DFARS does not now address the distinct software or firmware threat to cyber-active parts.

Larger defense contractors subject to the full coverage of these rules are required to have systems for counterfeit electronic parts avoidance and detection. A counterfeit electronic part detection and avoidance system shall include risk-based policies and procedures that address, at a minimum, the 12 criteria listed in Table 1.<sup>30</sup>

A database is currently used to report parts failure, as well as to collect and disseminate information on attributes of parts, components and materials, called the Government-Industry Data Exchange Program (GIDEP), a voluntary participation program that pre-dates the Internet. DoD presently relies upon GIDEP as the principal instrumentality to collect and disseminate reports on counterfeit electronics or other discrepant parts. GIDEP employs anachronistic methods to fulfill its important responsibilities because it has been underfunded and its mission has not evolved to align with expanding threats or to accelerate response. GIDEP does not employ large-scale data analytics and has no present ability to correlate incident- or attack-information to deployed equipment, and which could inform at-risk users.

In recent years, GIDEP has assumed increased importance as the principal vehicle by which defense contractors are to report suspect and confirmed counterfeit electronic parts. GIDEP has unfortunately not received the funding to modernize its information systems. As a result, the present utility of the GIDEP exchange is less than what could be achieved with a modern, data-driven system.<sup>31</sup>

Late in 2016, DoD also issued a final regulation that obligates all companies in the defense supply chain to promptly report “cyber incidents” with an actual or potentially adverse effect on an information system or information residing thereon.<sup>32</sup> This excludes commercial off the shelf suppliers, whose components often constitute the vast majority of weapons parts. The principal purpose of this regulation is to protect the confidentiality of covered defense information, at the moderate level, which as defined includes unclassified CTI of military and space significance.<sup>33</sup> Upon discovery of a cyber incident, the contractor is to report the incident to the Defense Industrial Base Network (DIBNet) portal.

---

30. Code of Federal Regulations, “Contractor Counterfeit Electronic Part Detection and Avoidance System,” Title 48, 252.246-7007(c).

31. Federal Acquisition Regulation (FAR) Case 2013-2, “Expanded Reporting of Nonconforming Items,” has been open for several years. A proposed FAR rule, published on June 10, 2016, would have significantly enlarged reporting of product and parts deficiency, for both civilian agencies and DoD, and would have expanded the role of GIDEP. 79 Fed. Reg. 33164 (Jun. 10, 2014.) The proposed rule has not been finalized, however.

32. Defense Federal Acquisition Regulation Supplement, “Network Penetration Reporting and Contracting for Cloud Services,” Federal Register 81, No. 204 [Oct. 21, 2016]: 72986. Available at: <https://www.gpo.gov/fdsys/pkg/FR-2016-10-21/pdf/2016-25315.pdf> (Accessed December 2016.)

33. Defense Federal Acquisition Regulation Supplement, “Safeguarding Covered Defense Information and Cyber Incident Reporting,” Subpart 252.204-7012 [Oct. 21, 2016]. Available at: <http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012> (Accessed January 2017.)

## Mitigating Potential Vulnerabilities

When the Contractor or subcontractors discover and isolate malicious software on the contractor's unclassified network in connection with a reported cyber incident, the contractor is required to submit

**Table 1: System Criteria to Detect Counterfeit Electronic Parts**

1.	The training of personnel.
2.	The inspection and testing of electronic parts, including criteria for acceptance and rejection. Tests and inspections shall be performed in accordance with accepted Government- and industry-recognized techniques. Selection of tests and inspections shall be based on minimizing risk to the Government. Determination of risk shall be based on the assessed probability of receiving a counterfeit electronic part; the probability that the inspection or test selected will detect a counterfeit electronic part; and the potential negative consequences of a counterfeit electronic part being installed (e.g., human safety, mission success) where such consequences are made known to the Contractor.
3.	Processes to abolish counterfeit parts proliferation.
4.	Risk-based processes that enable tracking of electronic parts from the original manufacturer to product acceptance by the Government, whether the electronic parts are supplied as discrete electronic parts or are contained in assemblies, in accordance with paragraph (c) of the clause at 252.246-7008, Sources of Electronic Parts.
5.	Use of suppliers in accordance with the DFARS section on <i>Sources of Electronic Parts</i> .
6.	Reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts. Reporting is required to the Contracting Officer and to the Government-Industry Data Exchange Program (GIDEP) when the Contractor becomes aware of, or has reason to suspect that, any electronic part or end item, component, part, or assembly containing electronic parts purchased by the DoD, or purchased by a Contractor for delivery to, or on behalf of, the DoD, contains counterfeit electronic parts or suspect counterfeit electronic parts. Counterfeit electronic parts and suspect counterfeit electronic parts shall not be returned to the seller or otherwise returned to the supply chain until such time that the parts are determined to be authentic.
7.	Methodologies to identify suspect counterfeit parts and to rapidly determine if a suspect counterfeit part is, in fact, counterfeit.
8.	Design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts. The Contractor may elect to use current Government- or industry-recognized standards to meet this requirement.
9.	Flow down of counterfeit detection and avoidance requirements, including applicable system criteria provided herein, to subcontractors at all levels in the supply chain that are responsible for buying or selling electronic parts or assemblies containing electronic parts, or for performing authentication testing.
10.	Process for keeping continually informed of current counterfeiting information and trends, including detection and avoidance techniques contained in appropriate industry standards, and using such information and techniques for continuously upgrading internal processes.
11.	Process for screening GIDEP reports and other credible sources of counterfeiting information to avoid the purchase or use of counterfeit electronic parts.
12.	Control of obsolete electronic parts in order to maximize the availability and use of authentic, originally designed, and qualified electronic parts throughout the product's life cycle.

the malicious software to the DoD Cyber Crime Center (DC3). Similarly, the Department of Homeland Security (DHS) operates the U.S. Computer Emergency Readiness Team (US-CERT) which serves many cyber security functions, such as: receipt and analysis of cyber event reports, dissemination of threat warnings, as well as promulgation of resources to identify, protect, detect, and respond to cyber threats.

---

**Mitigating Potential Vulnerabilities**

By enactment of the 2015 Cybersecurity Information Sharing Act (CISA), Congress authorized private companies to monitor and defend information systems and facilitated the voluntary sharing of cyber threat indicators and defensive measures with federal, state, and local government as well as with other companies.<sup>34</sup> To receive and disseminate information reported pursuant to CISA, DHS operates an Automated Indicator Sharing (AIS) system within the National Cybersecurity and Communications Integration Center (NCCIC).<sup>35</sup> DoD has its own voluntary reporting program, the Defense Industrial Base (DIB) Cybersecurity Program, by which DoD and DIB participants share cyber threat information in order to enhance the overall security of unclassified DIB networks and reduce damage to critical programs.<sup>36</sup>

Consequently, the task force observed the following with regard to the Department's ability to detect and report cyber-attacks:

- DoD programs, whether required or voluntary, do not regularly address the cyber threat to the software, firmware, and hardware of electronic systems embedded in the weapons systems upon which DoD relies.
- The required reporting of counterfeit electronics does not address either introduction of embedded malware, hardware Trojans, or other taints in electronic parts, and no present industry standard or "best practice" establishes means to isolate and identify malicious insertions or exploitation of latent vulnerabilities.
- The GIDEP system—largely form- and paper-based—is antiquated. It does not capture all suspect or confirmed counterfeits and does not employ data analytics to process and act upon large data sets. Nor is GIDEP either a prompt or assured method for dissemination of counterfeit information to potentially affected supply chain participants. It relies primarily upon manual decisions and submissions by participants (government and contractor) and upon individual review and reaction when alerts or advisories are issued.
- The "Safeguarding Covered Defense Information and Cyber Incident Reporting" rule and the DoD DIB cybersecurity programs focus on cyber events that threaten the confidentiality of protected types of information (especially CTI) and on threats to contractor information systems that result in exposure of that information.<sup>37</sup> These threats are distinct from those that hostile actors may execute against cyber-active systems, such as DoD's weapons systems where malicious code may compromise or alter the performance of penetrated systems.

DoD has not assigned the responsibility to aggregate, assess, characterize, or analyze supply chain attacks and there is no method presently in place to respond to and remediate such attacks, even when

---

34. Cybersecurity Information Sharing Act of 2015, S. 754, 114<sup>th</sup> Congress [2015].

35. Department of Homeland Security, "Automated Indicator Sharing (AIS)." *US-CERT*. Available at: <https://www.us-cert.gov/ais> (Accessed November 2016.)

36. DIB Cyber Incident Reporting & Cyber Threat Information Sharing Portal. Available at: <http://dibnet.dod.mil> (Accessed November 2016.)

37. Defense Federal Acquisition Regulation Supplement, "Safeguarding Covered Defense Information and Cyber Incident Reporting," Subpart 252.204-7012 [Oct. 21, 2016]. Available at: <http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012> (Accessed January 2017.)

## Mitigating Potential Vulnerabilities

known. The ability of DoD and its contractors must improve their ability to protect, detect, respond to, and recover from cyber-attacks on electronic components and systems in the supply chain.

### RECOMMENDATION 2

**USD(AT&L)** direct the **Deputy Assistant Secretary of Defense for Research (DASD(Research))** and the **Defense Advanced Research Projects Agency (DARPA)** to establish technical methods to identify discrepancies in software and firmware and for screening against malicious code or other hardware taints. This program should address:

- Continuous monitoring of critical systems and affordable sensors backed by advanced analytics.
- Technical approaches to obtaining trustworthy microelectronics from untrusted suppliers.
- Examination of various methods of tagging, monitoring, and authentication of integrated circuits.

---

There is little certainty as to whether the defense supply chain reports all counterfeit incidents. The reporting requirement is one of a dozen system criteria applicable to larger defense contractors and DoD does not explicitly require all defense supply chain participants to report counterfeit electronics. The current regulation does not clearly resolve who in the supply chain has reporting responsibility, and some contractors are believed to avoid reporting out of concern that they will suffer a stigma, reputational injury, or other adverse business consequences.

New or revised DFARS regulations are needed that establish criteria to identify supply chain cyber-attacks on software and firmware of electronic parts and systems that contain electronic parts. Further, all elements of the supply chain will need to adopt systems to mitigate these threats and to report such attacks to a DoD instrument.

### RECOMMENDATION 3

**USD(AT&L)** work to promulgate new regulations to eliminate the disincentives for industry self-reporting of counterfeits.

---

## 2.3 RESPONDING TO AND RECOVERING FROM ATTACKS

Similarly to *Detect*, few processes address the ability to *Respond* and *Recover* from corruption of the cyber supply chain. Cyber Awakening exercises are notable exceptions that highlight the difficulty of protecting current systems and the sobering consequences of cyber-attacks that exploit hardware and software vulnerabilities. The task force identified no routine training and few exercises that demonstrate how to fight through when an exploited vulnerability is detected.

---

## Mitigating Potential Vulnerabilities

For *Recovery*, the task force also found no training programs or exercises in restoring compromised systems or subsystems to a trusted status. In fact, DoD lacks visibility across programs to determine the applications in which parts are used, resulting in a slow, bottom-up process for replacing compromised parts or subsystems when a problem occurs. At present, information on problematic parts is shared via GIDEP, which is historically slow in getting actionable information to those who need it. Urgent needs are addressed by email advising each program office to check on whether the problematic part affects their system.<sup>38</sup>

A further issue is that present regulations do not produce prompt reporting. A recently revised regulation extends a “safe harbor” for costs of counterfeit parts, which otherwise might be unallowable, upon satisfaction of several conditions (e.g., “timely” written notice to the cognizant contracting officer and GIDEP). Under the regulation, “timely” is set at “within 60 days after the contractor becomes aware”.<sup>39</sup> Even after initial notice, GIDEP likely will take further time before it issues a suspect counterfeit report. Even then, the GIDEP report may not reach persons who have the necessary knowledge or authority to act. Considered as a whole, GIDEP is not certain to capture a high percentage of suspect or confirmed counterfeits and is not coupled with instrumentalities to rapidly communicate event information to potentially at-risk users.

### RECOMMENDATION 4

**USD(AT&L)** direct the Defense Standardization program office to modernize the GIDEP reporting system and extend GIDEP to provide information to the JFAC:

- Enhance GIDEP’s functionality, funding, and staffing to include enhanced capability to rapidly communicate on vulnerability, events, and mitigation to users of parts that are under attack or at risk.
- Expand GIDEP’s charter to encompass reports of software and firmware attack as well as hardware.
- GIDEP should inform JFAC of counterfeit components by automated means.

---

38. Further information on GIDEP duties and responsibilities is available at:  
<http://www.gidep.org/about/opmanual/chap04.pdf> (Accessed December 2016.)

39. Code of Federal Regulations, “Costs related to counterfeit electronic parts and suspect counterfeit electronic parts,” Title 48, 231.205-71(b)(3).



## Chapter 3: Approaching Acquisition Differently

### 3.1 IMPROVING PROGRAM PROTECTION PLANS

In 2011, Program Protection Plans were instituted as a forward-looking mechanism to improve cyber supply chain posture. The purpose of the PPP is to help programs ensure that they adequately protect their technology, components, and information. This includes information that alone might not be damaging and might be unclassified, but that in combination with other information could allow an adversary to clone, counter, or defeat warfighting capability.<sup>40</sup> PPPs were designed to guide the program office in updating their security measures as threats and vulnerabilities change. This can result in a templated activity that requires modest preparation to proceed through acquisition milestones for new acquisition programs. There are several problematic aspects of this approach:

- The quality and depth of PPPs varies widely and pressure to gain milestone approval incentivizes limited scope and depth of PPPs;
- Protection narrowly focuses on criticality and there is no consistency in its definition;
- PPPs do not address design elements calculated to provide full system security;
- Program Executive Offices (PEOs) and program manager (PM) staffs lack the cyber expertise needed for effective systems engineering and program protection planning;
- PPPs do not incorporate effective third-party security review of systems and fail to provide for ongoing security review and risk analysis in sustainment or provide a mechanism to react to newly discovered attacks; and
- PPPs do not incorporate measures calculated to adequately inform operators of risk or failure modes or their consequences and do not incorporate provisions allowing operators to fight through failures caused by supply chain or other cyber-attacks.

To define critical components, programs identified key mission elements, yet there were no consistent definitions of such elements. For example, critical components in some plans on air platforms were identified as only those that threatened the life and safety of the crew. While life safety is certainly important as an organizing framework, it completely fails to account for overall mission success. In other words, the PPP (in this case) confined itself to a very narrow aspect of the mission, thereby curtailing its effect on overall program protection and supply chain quality.

---

40. Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)), *Program Protection Outline & Guidance*, Version 1.0, July, 2011.



---

## Approaching Acquisition Differently

### LIMITATIONS OF THE CURRENT PPP PROCESS

Because the early cyber supply chain PPP guidance was procedural, it was often viewed as a compliance measure that was assigned to a low-level staffer whose goal was to prevent system delays. Critical component lists are often very large, thus making it difficult to reduce risk on a part-by-part basis. Even highly qualified suppliers with extensively vetted employees incorporate parts from global suppliers who are not vetted and whose parts are seldom understood. These integrating suppliers have little control over, and often far too little knowledge of, the operation of these component parts to assess supply chain risk. Specification was often limited to “replaceable units,” which meant that there is no bill of materials comprehensive enough to identify vulnerable parts, much less consideration related to resilient design of those parts. Commercial entities often have more extensive knowledge of commonly used parts, while in DoD, there is often only rudimentary analysis of how common embedded parts (e.g., microcontroller, memory, sensor) might provide an easy supply chain attack vector for the resulting system.<sup>41</sup>

PPPs seldom considered “designed-in” safety measures like monitoring, encapsulated design, and interfaces that would allow rapid substitution of suspect components or design diversity that may greatly improve cyber supply chain resilience. Because subcomponents are not well known, parts with existing vulnerabilities might easily be used. Once such vulnerabilities are identified (given the absence of a comprehensive bill of materials), it is difficult to quickly find out what systems have incorporated the suspect part.

The PPP process would also benefit from mandated security design review. Such a review could identify subsystems that may benefit from redundant independent components and continue to operate even if a single component were compromised. The resulting systems might inadvertently have huge, relatively unknown attack surfaces; any one of which, if compromised, would prevent successful completion of a critical mission. PPPs often do not specify design elements that would provide the ability to easily upgrade or change systems during operation or maintenance. Consequently, the most powerful techniques for protecting systems from supply chain attacks (i.e., designed in resilience, agility, and self-monitoring) are not usually considered in PPPs.

The situation with lifecycle protection is even more constrained. Often no provision is made for “in operation” assessment of cyber supply chain attacks. While it is understood that the best designed systems will require changes as vulnerabilities and attacks are discovered, few DoD systems have designed-in capabilities for operational remediation.

---

41. Note the historical change—When DoD specified and developed all the components of a weapons system and did not generally use preexisting commercially available parts, DoD had detailed knowledge of each of these parts often to the exclusion of others.

## Approaching Acquisition Differently

### RECOMMENDATION 5

**USD(AT&L)** ensure that DoDI 5000.02 makes secure design and realistic risk assessment a core element of PPPs:

- Each program manager should develop a rigorous security model (naming potential attacks) for weapons systems during specification with mandatory analysis of efficacy verifying that design and implementation will meet security requirements with high assurance
  - Each program manager should incorporate funded in-depth security review of critical systems at key points pre-initial operational capability and during operations with the aims of remediating security flaws and improving acquisition, engineering, operational, or sustainment security. Such reviews should be conducted by a specialized organization or organizations to be established in or endorsed by JFAC.
- 

Supply chain resilience was never identified in PPPs in a manner that preferred these designs over less resilient alternatives. Resilience to supply chain attacks was not a selection criterion anticipated by PPPs and there is limited scope to introduce supply chain resilience and analysis after initial production.

### RECOMMENDATION 6

**USD(AT&L)** ensure that DoDI 5000.02 anticipates the need for resilience, ongoing evaluation, and upgrade:

- Each program manager should specify design elements supporting resiliency including well defined interfaces for encapsulated subsystem allowing substitution of alternate or newly hardened implementations as well as procedures and testing to ensure the viability of substitution and upgrade.
  - Each program manager should establish design elements and processes to identify and replace parts or subsystems with known or recently discovered vulnerabilities.
- 

### LOOKING FORWARD

The task force recommends that PPPs be transformed into a comprehensive document governing the security of critical weapons systems throughout their lifetime to specifically address resilient design, cyber assessment (red teaming) at each phase of weapon development and deployment, mechanisms supporting remediation (including rapid upgrade), monitoring, and vulnerability assessment. It is also important to note that the DoD recently issued Enclosure 14 in DoDI 5000.2, "Cybersecurity in the Defense Acquisition System," that can broadly be applied to cyber supply chain design, evaluation,

---

### Approaching Acquisition Differently

maintenance and deployment.<sup>42</sup> The enclosure provides comprehensive, practical and effective guidance that can be usefully applied to cyber supply chain. With the issuance of the enclosure, PPPs can become the comprehensive, lifetime vehicle to ensure broad program protection and supply chain resilience. The PPP should thus support the full range of protective activities such as:

- Secure, diverse design through safe manufacture;
- Comprehensive system evaluation (including all parts in a system);
- Monitoring interfaces;
- Comprehensive part characterization and access to up-to-the-minute vulnerability information on parts and subsystems;<sup>43</sup>
- Part integrity protection from suppliers to operations; and
- Training activities for operators, maintenance staff and acquisition staff.

All of these activities should be supported by expert security design and review as well as informed red teaming throughout the system lifetime from design to retirement.

PPPs also need to consider potential parts obsolescence, as well as encapsulated and modular system designs so that better protected, more capable subsystems can be adopted quickly when they are available in related military or commercial systems.

### RECOMMENDATION 7

**USD(AT&L)** promote PPPs that encompass cradle to grave protection for new and existing systems:

- The Assistant Secretary of Defense for Logistics and Materiel Readiness (ASD(L&MR)) should revise the Logistics Assessment Guide to include program protection as one of the areas to be reviewed periodically after initial operational capability (IOC).
- Each PPP should be transitioned to the program manager responsible for sustainment and disposal.

---

Responsibility for comprehensive PPPs must reside with the program manager and endure throughout program lifetime. Program managers must receive adequate training, be supported by experts who are able to evaluate PPPs and then be informed by active red team initiatives throughout design, manufacture, deployment, and use. PMs must also be able to select, in a cost-effective manner,

---

42. USD(AT&L), *Cybersecurity in the Defense Acquisition System*, DoD Instruction 5000.02, January 26, 2017, Enclosure 14 pg. 170.

43. The task force emphasized that access to detailed part information, including ongoing vulnerability discoveries, be made part of the selection criteria for PPP supported acquisitions.

---

## Approaching Acquisition Differently

proposals which include differentiated protection for their program's systems and subsystems. PPPs must provide remediation procedures and training for operators, maintenance staff, and acquisition activities throughout system lifetime. Similarly, the same training must also be afforded to diverse suppliers who incorporate automated measures calculated to guarantee shipment integrity from original manufacturers throughout a system's lifetime. Due to the nature of rapid, unexpected upgrades that degrade the ability of well-resourced adversaries to target critical systems, operational procedures should ensure that the upgrades are performed and documented in a timely manner.

Maintenance staffs, on occasion, were discovered to have innocently reduced cyber supply chain safety in an effort to simplify procedures. So it is important that the PPPs explicitly provide for ongoing education (derived from ongoing assessments) to operational and maintenance staff.

### RECOMMENDATION 8

**USD(AT&L)** explore avenues to improve training and standards:

- The Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)) should set standards for criticality that are appropriate for mission assurance.
- Program managers responsible for PPPs should complete training (such as DAU ACQ 160) prior to taking command.

---

## 3.2 SUPPLIER VETTING

DoD depends upon a global supply chain, but it executes key defense programs through prime contracts with a relatively small number of cleared DIB suppliers. At the prime contract level, DoD has leverage to apply controls upon the selection of suppliers and on the use of supplier assurance measures. Cyber supply chain security requires “end-to-end” attention throughout the product lifecycle. Increasing emphasis is placed upon systems security engineering such as the new National Institute for Standards and Technology (NIST) Special Publication (SP) 800-160 as well as standards for systems and software engineering published by International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and other bodies.<sup>44</sup> The acquisition process figures prominently in systems security engineering. The qualification and selection of suppliers is an important dimension to systems security.

Supplier vetting includes several distinct considerations that contribute to trustworthiness and reliability. Many factors can be considered: e.g., ownership and control of the supplier, financial stability, historical record of delivery, reports to GIDEP or similar organizations, and data on compliance and ethical business conduct. Much of this information is accessible from publicly available sources. DoD has

---

44. NIST Special Publication 800-160, “Systems Security Engineering,” [November 2016]. Available at: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf> (Accessed December 2016.)

### Approaching Acquisition Differently

unique access to information that can be important or even decisive in the vetting process. It has the authority to collect and act on intelligence-source information to consider supply chain risk. For certain specified types of national security procurements, the Department already has the legal authority to exclude sources if they are deemed hazardous on the basis of intelligence information to present “supply chain risk.”<sup>45</sup>

Especially for sustainment of fielded systems, it sometimes is necessary to purchase an electronic part from other than the OEM or its authorized distributor. The current DFARS that concern counterfeit electronic parts now authorize contractors to qualify “contractor-approved suppliers” and to purchase parts from other, even higher risk suppliers.<sup>46</sup> The regulation relies on manual processes imposed upon individual contractors and on measures of inspection, testing, and authentication at the component level.

Cyber supply chain vulnerability can be enabled and aggravated if adversaries are able to penetrate contractor information systems and exfiltrate technical information about DoD systems and capabilities. Cyber espionage injures important national security interests; the consequences of such attacks can inform hostile parties of vulnerabilities in the supply chain for particular parts and systems. These risks extend beyond the higher tiers of DoD contractors, who likely have good cyber safeguards, to lower tiers of the supply chain, including commercial suppliers and small business. DoD already requires suppliers subject to the “Safeguarding Covered Defense Information and Cyber Incident Reporting” DFARS to safeguard unclassified CTI using the new NIST SP 800-171, created for use to protect forms of controlled unclassified information on nonfederal systems.

Other observations include:

- Program offices rely upon prime contractors to identify critical components and to submit requests to DIA to perform threat assessments on these suppliers;
- DoD Components do not routinely impose systems security engineering requirements upon contractors;
- Contractor approaches to vetting suppliers for supply chain risk vary greatly producing the risk of inconsistent result to purchasing DoD components;
- The manual process now authorized for approving “contractor-approved suppliers” and parts from other sources is an inefficient way to ensure authenticity and protect against counterfeit or tainted electronic parts; and

---

45. *NDAA for Fiscal Year 2011*, Public Law 111-383 [January 2011], Section 806. The source of this exclusion authority, defines “supply chain risk” as “the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

46. Code of Federal Regulations, “Contractor Liability for Loss of or Damage to Property of the Government,” Title 48, 246.870(a)(1)(ii) and (iii).

---

## Approaching Acquisition Differently

- Vetting of suppliers should encompass review and assessment of their cyber safeguards to protect CTI and other forms of sensitive unclassified information against unauthorized access.

### RECOMMENDATION 9

**DIA coordinate with JAPEC** to focus its resources on specific targeted, adversarial collection activities.

---

Prior to the 2011, the guidance for program managers to develop a program protection plan was contained in DoD Directive 5200.39, “Security, Intelligence, and Counterintelligence Support to Acquisition” issued by Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)) in 1994.

The requirements from 1994 articulated that the PPP served as the single source document used to coordinate and integrate all of the protection efforts designed to deny foreign collection activities and prevent inadvertent disclosure, where the focus of what needed to be protected was Critical Program Information and the program manager relied on the Multi-Discipline Counterintelligence threat assessment as the primary threat assessment report. The process and its artifact, the PPP, emphasized protecting advanced research and technology from unauthorized or inadvertent disclosure; for example, if a weapon system derived a capability advantage from some leading-edge technology, algorithm, or component, that critical program information (CPI) was closely guarded through process and technical means. Today, DIA produces intelligence and counterintelligence assessments, to include the technology targeting risk assessments (TTRAs), to help DoD Components identify threats to CPI.<sup>47</sup>

Additionally, DoDI 5200.44, “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks,” states that DIA is responsible for producing an intelligence and counterintelligence assessment of supplier threats to acquisition programs providing critical weapons, information systems, or service capabilities.<sup>48</sup> This provenance-based vetting process is time consuming and has delayed project milestones in many cases. Furthermore, even in cases where suspicious influence was detected, projects often did not change suppliers because of cost, limited availability of qualified suppliers, or delays. The Undersecretary of Defense for Intelligence (USD(I)) can strengthen this process by contracting for commercial due diligence. This will incentivize companies to adhere to approved standards that will decrease the potential access to critical information by adversaries.

---

47. USD(I)/USD(AT&L). “Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E),” DoDI 5200.39.

48. DoD CIO/USD(AT&L), “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks,” DoDI 5200.44.

---

**Approaching Acquisition Differently**

**RECOMMENDATION 10**

**USD(I)** enhance current DIA supplier vetting by contracting for commercial due diligence.

---

### **3.3 SUPPORTING PROGRAM OFFICES TO IMPROVE ASSURANCE**

Prior sections have addressed several aspects of program protection, including risk assessment, supplier vetting, and system design. Achieving an appropriate level of supply chain cybersecurity for DoD systems requires that these elements be addressed. However, effective cybersecurity goes beyond these high-level aspects of program protection. Cybersecurity must also be a key consideration during the development and testing of DoD systems. This section introduces aspects of cybersecurity that must be addressed during system development and testing, and recommends approaches to ensure that program offices can address these aspects effectively.

The term assurance refers to confidence—on the part of developers, acquirers, and operators—that a system’s hardware and software can achieve a desired degree of security and resilience even in the face of attempts to introduce flawed components, malicious inputs to operational systems, or other forms of attack. Such confidence stems from the measures taken during the design, implementation, and testing of the system. The Program Protection Plan Outline and Guidance refers to the need for software assurance.<sup>49</sup> Unfortunately, this guidance provides minimal direction about the measures that lead to sufficient assurance or how to implement them. Program offices and prime contractors have largely been left on their own to devise and implement approaches to assurance.

#### **JOINT FEDERATED ASSURANCE CENTER**

In February 2015, the Deputy Secretary of Defense created the JFAC in response to language in the FY 2014 National Defense Authorization Act (NDAA) that required DoD to “establish a joint federation of capabilities to support trusted defense system needs to ensure the security of software and hardware developed, acquired, maintained, and used by DoD.”<sup>50</sup>

JFAC is led by a steering committee with members representing the office of the Secretary of Defense (AT&L and DoD Chief Information Officer (CIO)), the military departments, Missile Defense Agency (MDA), National Security Agency (NSA), National Reconnaissance Office (NRO), Defense Information Systems Agency (DISA), and Defense Microelectronics Activity (DMEA). The functions of JFAC are to promote and facilitate hardware and software assurance capabilities in support of program offices and other DoD and U.S. Government organizations. The JFAC charter emphasizes developing an inventory of hardware and software assurance resources—vulnerability analysis tools in particular—across the Department. Such an inventory raises awareness of these tools as well as enhances the

---

49. DASD(SE), Program Protection Outline & Guidance, Version 1.0, [July, 2011].

50. NDAA for Fiscal Year 2014, Public Law 113–66 [December 2013], Section 937.



## Approaching Acquisition Differently

processes for applying them. JFAC serves as the DoD contact for interagency efforts related to hardware and software assurance, and individual members conduct varying amounts of research, tool development and evaluation, and support of program offices.

While JFAC provides DoD with a central source of expertise on hardware and software assurance, its establishment as a “federation” means that it does not have authority, resources, or capability of its own. The ability of JFAC to support program offices and help improve the assurance of DoD hardware and software is entirely dependent on the voluntary commitment of JFAC member organizations. Given that each member has its own sources of management direction, funding, and priorities independent of JFAC, it is unlikely that JFAC will provide actual support to program offices, although individual JFAC members may provide some level of support to program offices that report to their respective DoD Component.

DoD Components that are members of JFAC play varying roles in hardware and software assurance. Research organizations evaluate current approaches and tools, and conduct or sponsor exploration of new approaches to improving assurance. In-house development organizations may establish standardized guidance for achieving desired levels of assurance, and acquisition agencies may establish common procurement language to require that contractors consider assurance during the development of new systems. However, there is no DoD-wide approach to assurance. JFAC provides a vehicle for creating interagency efforts and sharing approaches and results but nothing in the JFAC charter ensures that such efforts or sharing will occur, or that they will benefit program offices.

### ACHIEVING ASSURANCE

Over the last fifteen years, commercial vendors and commercial end users have come under increasing pressure to improve the assurance of the hardware and software that they create. This pressure has resulted from the highly visible increase in cyber-attacks and from customers’ pressure to improve resistance to attack. In response to these pressures, many organizations have created in-house programs focused on assurance.<sup>51, 52</sup>

While these assurance programs vary from company to company, most share some common attributes:

- Rather than allowing (or requiring) individual development teams to select their own approaches to assurance, they standardize an enterprise-wide approach (with appropriate adaptations for different classes of systems and technology);
- They address both product design and product implementation;

---

51. Gary McGraw, Sammy Migues, and Jacob West, *Building Security In Maturity Model (BSIMM) Version 7*, [San Francisco, California: Creative Commons, 2016]. Available at: <https://www.bsimm.com> (Accessed December 2016.)

52. Software Assurance Forum for Excellence in Code (SAFECode), “Principles for Software Assurance Assessment: A Framework for Examining the Secure Development Processes of Commercial Technology Providers,” [2015]. Available at: [https://www.safecode.org/publication/SAFECode\\_Principles\\_for\\_Software\\_Assurance\\_Assessment.pdf](https://www.safecode.org/publication/SAFECode_Principles_for_Software_Assurance_Assessment.pdf) (Accessed October 2016.)



---

### Approaching Acquisition Differently

- They depend heavily on the use of security scanning and testing tools of the sort that JFAC charter refers to. Typically, an organization will select a suite of tools and provide its developers with specific guidance as to what tool-reported problems are “must fix;”
- They incorporate a central assurance team that advises individual development teams and ensure that they are in fact implementing the common approach to assurance;
- They consider assurance a mandatory rather than a discretionary product attribute. Any deviations from requirements are subject to appropriate levels of management review; and
- They are updated periodically to reflect the existence of new kinds of attacks and the availability of new and more effective tools.

While no such assurance program has enabled an organization to achieve perfect security, mature programs have resulted in improved security. Evidence of such improvements is provided by the growing adoption of assurance programs and by sophisticated customers’ insistence that their suppliers implement such programs.<sup>53, 54</sup>

#### RECOMMENDATION 11

**Deputy Secretary of Defense** update the JFAC charter to:

- Establish JFAC as a DoD-wide hardware and software assurance organization with a mandate to support Program Management Offices, Program Executive Offices, and sustainment activities.
- Develop prescriptive standards and requirements for hardware and software assurance processes and tools.
- Provide the program manager and the JFAC Steering Committee with an independent perspective on risk articulated by a peer-level official in JFAC in cases where a program is unable to adhere to standards or requirements.

---

Updating the JFAC charter will enable it to deliver effectively on the Congressional direction to “support trusted defense system needs to ensure the security of software and hardware developed, acquired, maintained, and used by DoD.”<sup>55</sup> This transformation, will clarify the source of authoritative guidance on hardware and software assurance in DoD. It will also replace a loose confederation of

---

53. Gary McGraw, Sammy Migues, and Jacob West, *Building Security In Maturity Model (BSIMM) Version 7*, [San Francisco, California: Creative Commons, 2016]. Available at: <https://www.bsimm.com> (Accessed December 2016.)

54. Financial Services Information Sharing and Analysis Center, “Appropriate Software Security Control Types for Third Party Service and Product Providers,” v. 2.3 [October 2015]. Available at: <https://www.fsisac.com/sites/default/files/news/Appropriate%20Software%20Security%20Control%20Types%20for%20Third%20Party%20Service%20and%20Product%20Providers.pdf> (Accessed December 2016.)

55. *NDAA for Fiscal Year 2014*, Public Law 113–66 [December 2013], Section 937.

### **Approaching Acquisition Differently**

independent organizations, each pursuing its own agenda, with an effective organization that is well-positioned to support program offices.

Because cybersecurity is a dynamic field in which new kinds of systems are constantly being developed and in which attackers are constantly devising new techniques for undermining system security, it will not be possible for JFAC to issue a single set of standards and requirements that will remain effective forever. As illustrated in Figure 5, JFAC should monitor the cybersecurity landscape on an ongoing basis and update standards and requirements as appropriate, either because new kinds of attacks are discovered or because new security tools or techniques are created. The hardware and software assurance standards that program offices must follow should be updated periodically (likely annually) and put into effect after an appropriate transition period.

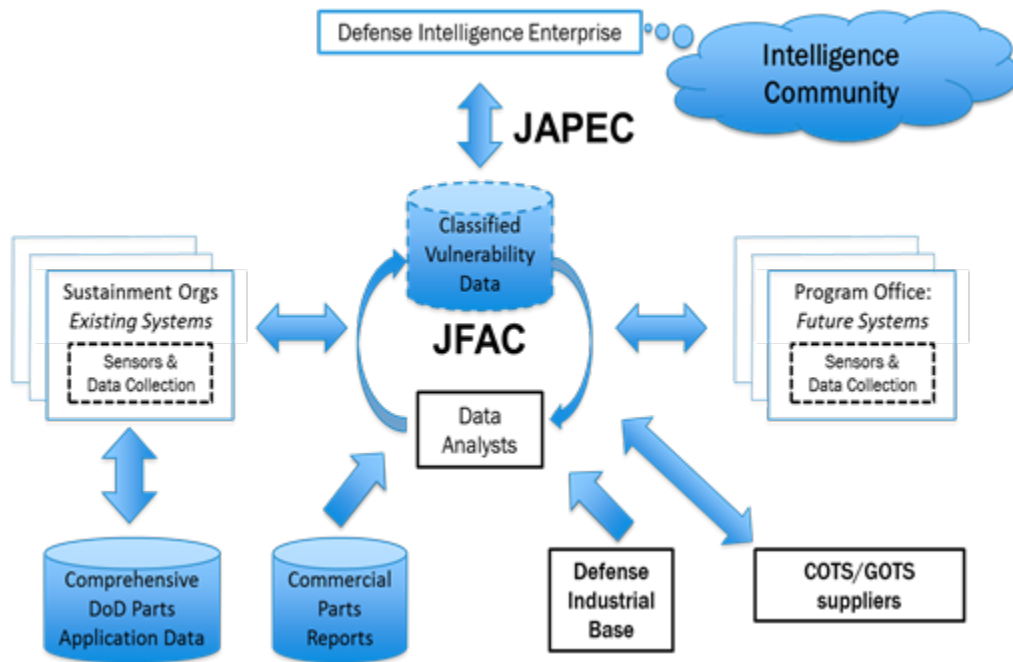
In the same way, the JAPEC will report new trends in threat and attacker techniques and be a critical input to the process of updating standards and requirements. Through integrated analysis done at the enterprise level, JAPEC consolidates existing acquisition, law enforcement, counter intelligence, and intelligence community information to connect the dots in reducing risk, thus linking blue priorities with adversary targeting and activity.

#### **RECOMMENDATION 12**

**USD(AT&L) and USD(I)** charter, fund, and staff JAPEC to:

- Coordinate intelligence collection requirements for acquisition programs
  - Coordinate and provide briefings of specific threat activities to targeted programs
-

## Approaching Acquisition Differently



**Figure 5:** Recommended JAPEC and JFAC roles to enhance shared supply chain situational awareness.

Given the difficulty of achieving hardware and software assurance and the scarcity of expertise in this challenging domain, it is unrealistic to expect each program office to devise its own approach to assurance. By establishing JFAC as a central source of expertise and requiring it to create prescriptive standards and guidance, DoD will both improve hardware and software assurance and simplify the task of program offices.

The difficulty of achieving hardware and software assurance, combined with the complexity and demanding requirements of defense systems, makes it unlikely that every program office will be able to comply with every standard and requirement that JFAC issues. When an exception appears necessary, JFAC personnel should work with the program office to understand the challenges and the implications of the exception, and then ensure that an appropriate level of management in the program office is briefed by a peer level official from JFAC on the implications of the exception. While the program manager bears ultimate authority and responsibility for the approving the exception, a clear and credible explanation of the risk being accepted and its implications will result in better program manager decisions, and higher levels of hardware and software assurance. JFAC should also review any proposed exception to determine whether it demonstrates a need for improved processes, tools, or training, and make appropriate updates.

USD(AT&L) guidance should make it clear to program offices that they must adhere to the standards and requirements that the JFAC issues, and must cooperate with the JFAC process for reviewing any exceptions as described in the previous recommendation. In addition, because hardware and software

---

## Approaching Acquisition Differently

assurance are often challenging problems, program offices should be advised to seek input from JFAC at key points during the program lifecycle. For example, it may be appropriate to seek JFAC input to proposal evaluation if a contractor proposes a tool or approach to software assurance whose use is not addressed by JFAC standards or requirements.

### RECOMMENDATION 13

**USD(AT&L)** issue guidance to programs to work with JFAC and ensure adequate funding and authority for the JFAC mission.

---

## 3.4 CYBERSECURITY FOR COMMERCIAL AND OPEN SOURCE COMPONENTS

DoD makes extensive use of commercial-off-the-shelf (COTS) hardware and software, and open source software (OSS) systems, as well as open source hardware components and subsystems. COTS and OSS appear where defense systems incorporate information processing subsystems (such as for data reduction, storage, or display) and as embedded computing components of operational systems (such as avionics maintenance consoles and hull, mechanical, and electrical subsystems of naval vessels). Command, control, communications, computing, intelligence, surveillance and reconnaissance (C4ISR) systems rely heavily on COTS and OSS, and emphasis on affordability often pushes suppliers to use COTS.<sup>56</sup>

COTS and OSS developers primarily seek to serve the broad commercial marketplace. Many innovations in computing technology become available in COTS and OSS, and rapid updates are common as developers seek new ways to attract users and appeal to broader markets. While COTS and OSS developers are happy to see DoD buy and use their products, DoD applications represent only a small fraction, less than one percent, of the market for COTS and OSS products.<sup>57</sup> While information technology components embedded in weapons systems are not part of that budget, total DoD spending on information technology is still a small fraction of total U.S. or worldwide spending.<sup>58</sup>

Many forms of COTS technology are dependent on a global supply chain, creating an opportunity for “upstream” sources to introduce unwanted functionality into hardware, firmware, or software. Similar vulnerabilities accompany OSS products where complex code can include elements from many sources both known and unknown. Advanced adversaries can exploit their influence over COTS and OSS

---

56. Bloomberg Government, “DoD in ‘knife fight’ over supply chain, security chief says,” [November 4, 2016]. Available at: <https://about.bgov.com/blog/dod-knife-fight-supply-chain-security-chief-says> (Accessed November 2016.)

57. Richard W. Walker, “Federal IT Spending Slashed In Proposed 2015 Budget,” *Information Week*, [March 5, 2014]. Available at: <http://www.informationweek.com/government/cybersecurity/federal-it-spending-slashed-in-proposed-2015-budget/d/d-id/1114126> (Accessed October 2016.)

58. Select USA, “Software and Information Technology Spotlight.” Available at: <https://www.selectusa.gov/software-and-information-technology-services-industry-united-states> (Accessed November 2016.)

---

## Approaching Acquisition Differently

software to sabotage equipment, insert malicious code, or otherwise subvert the functionality and trustworthiness of military equipment.

Inadequate cybersecurity of COTS or OSS products used in DoD applications can expose the defense system to attacks with potentially serious consequences. Like DoD, commercial customers are concerned about cybersecurity. Some leading commercial companies have implemented strong measures to vet sources and actively manage their supply chain risk.<sup>59</sup> Others are working with standards-setting organizations to obligate their suppliers to improve software security measures.<sup>60</sup> Adoption of secure development and supply chain practices in response to (primarily commercial) customer pressures has been uneven, however. Some COTS vendors have adopted secure development and supply chain practices while others have not.<sup>61</sup> OSS developers have recently begun to focus on security, but these efforts are still a work in progress.<sup>62</sup>

### SECURITY STANDARDS

A few consensus standards dealing with secure development and supply chain security for COTS and OSS hardware and software are emerging, but compliance with these standards is not yet widespread. The DoD CIO has been involved in the creation of the Open Group's Open Trusted Technology Provider™ Standard (O-TTPS) which is now recognized as ISO Standard 20243, "Mitigating Maliciously Tainted and Counterfeit Products." DoD CIO has also participated in the ISO working group responsible for ISO Standard 27036, "Information Security for Supplier Relationships." NSA's National Information Assurance Partnership (NIAP) has participated in the ISO working group that created ISO Standard 27034, "Information Technology – Security Techniques – Application Security," which focuses on secure development practices. However, DoD has not attempted to compel COTS and OSS developers to conform with any of these standards. Nor has DoD imposed upon its contractors any obligation that they employ supply chain risk management practices specifically aimed at COTS and OSS risks.<sup>63</sup>

---

59. NIST, "Best Practices in Cyber Supply Chain Risk Management" (referencing case studies of companies such as Intel, Boeing-Exostar, Cisco, etc.), [2015]. Available at: <http://usresilienceproject.org/best-practices/supply-chain-resilience/> (Accessed October 2016.)

60. Financial Services Information Sharing and Analysis Center, "Appropriate Software Security Control Types for Third Party Service and Product Providers," v. 2.3 [October 2015]. Available at: <https://www.fsisac.com/sites/default/files/news/Appropriate%20Software%20Security%20Control%20Types%20for%20Third%20Party%20Service%20and%20Product%20Providers.pdf> (Accessed December 2016.)

61. Software Assurance Forum for Excellence in Code (SAFECode), "Principles for Software Assurance Assessment: A Framework for Examining the Secure Development Processes of Commercial Technology Providers," [2015]. Available at: [https://www.safecode.org/publication/SAFECode\\_Principles\\_for\\_Software\\_Assurance\\_Assessment.pdf](https://www.safecode.org/publication/SAFECode_Principles_for_Software_Assurance_Assessment.pdf) (Accessed October 2016.)

62. The Linux Foundation is sponsoring a collaborative "Core Infrastructure Initiative" (CII) to address open-source software security. Available at: <https://www.coreinfrastructure.org/> (Accessed October 2016.)

63. For information and communications technology products, federal civilian agencies are encouraged to use NIST Special Publication (SP) 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations." Available at: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf> (Accessed October 2016.)

## Approaching Acquisition Differently

### INFLUENCING COTS AND OPEN SOURCE SOFTWARE DEVELOPERS

Given the broad commercial market for COTS and OSS, DoD has modest leverage over COTS supplier practices. To the extent that the commercial market demands that developers deliver secure products, the Department should encourage and participate in such industry efforts to promote secure product design. Furthermore, DoD frequently has less access and expertise with respect to design, manufacturing, and evaluation of COTS parts than equally large or larger commercial purchasers. Such comprehensive knowledge is mandatory to understand and thoughtfully use commercial parts. DoD would benefit from a comprehensive program to understand critical design information in COTS parts as a participant in a cooperative industry initiative to understand these parts and systems.

Developers may find commercial market pressure to deliver secure products to be more compelling than attempts by DoD to mandate change which may jeopardize access to commercial sources for whom there may be no ready substitute. While the government has processes for evaluating some aspects of the security of COTS and OSS (e.g., Common Criteria evaluation of product security features and Federal Information Processing Standard (FIPS) 140, evaluation of cryptographic products or components), no DoD program exists to evaluate the secure development or supply chain management practices of COTS or OSS products or is able to recognize such practices based on their compliance with industry standards.

### VULNERABILITY REPORTING AND RESPONSE

Almost all COTS and OSS developers must deal with reports of security vulnerabilities in their products. Such reports primarily focus on software vulnerabilities, and developers respond to them by releasing security updates (patches) for customers to install. Because vulnerabilities are very common, almost all developers have established response processes although the timeliness and quality of responses vary among developers.

Hardware vulnerabilities are much less common than software vulnerabilities, but they do occur frequently enough to be a concern for users of COTS hardware. Hardware vulnerabilities may also pose challenging response problems. While it is usually feasible to update embedded firmware, vulnerabilities in hardware components may require modification or replacement of the hardware. Beginning in the early 1990s, the CERT Coordination Center (and more recently the US-CERT) has maintained a database that tracks reported software vulnerabilities and a mailing list that advises users of vulnerabilities and vendor responses to them. DoD Components respond to vulnerability advisories through the Information Assurance Vulnerability Alert (IAVA) process.<sup>64</sup> US-CERT does not track hardware vulnerabilities and there is no consolidated database or alerting process for hardware vulnerabilities akin to the established process for software vulnerabilities.

While not as common as software vulnerabilities, COTS hardware vulnerabilities have been reported and can have significant impact on the security of systems that incorporate affected products or

---

64. Chairman of the Joint Chiefs of Staff Instruction, Information Assurance (IA) and Support to Computer Network Defense (CND), CJCSI 6510.01F, [June 2015]. Available at: [http://www.dtic.mil/cjcs\\_directives/cdata/unlimit/6510\\_01.pdf](http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf) (Accessed November 2016.)

### Approaching Acquisition Differently

components. DoD programs and end users of COTS products would benefit from timely awareness of such vulnerabilities. It is appropriate for DoD to take the lead in establishing a Hardware CERT just as it did in establishing the CERT Coordination Center in the early 1990s. As the scope of Program Protection Plans is extended into system sustainment, advisories from the Hardware CERT will serve as a key resource that enables program offices and operational users to take action to protect their systems. Acquisition tools can be used to encourage or even require DoD contractors to report on hardware vulnerabilities, along the lines of the DFARS regulations now in place that concern counterfeit electronic parts.

#### RECOMMENDATION 14

**USD(AT&L)** direct the establishment of a Hardware Computer Emergency Readiness Team (CERT) to track the reporting and remediation of vulnerabilities in COTS hardware and embedded firmware.

---

While DoD has limited influence over the practices of COTS and OSS developers, experience with Common Criteria and FIPS 140 shows that developers are willing to make some investments to meet DoD requirements. This result is rendered more likely if the requirements align with commercial objectives and accommodate methods and techniques that are not “federal-centric” or “federal-specific.” The emergence of secure development and supply chain management practices, and their adoption by some COTS and OSS developers, is a trend that is valued by commercial customers and has the potential to benefit the Department.

DoD can benefit by understanding emerging trends and standards, influencing them where appropriate, and then incorporating them as requirements for acquisition of COTS and OSS products. The preexisting engagement of DoD CIO and NIAP with the ISO and Open Group standards bodies responsible for secure development and supply chain security standards provides a good starting point for the adoption of such requirements. DoD may wish to engage with the Linux Foundation Core Infrastructure Initiative in order to understand, and potentially influence, standard security practices for OSS development.

The Department is most likely to secure its objectives if COTS and OSS suppliers adopt strong measures of commercial origin that benefit their brand and market position. As an alternative, DoD may choose to create its own standards for secure development and supply chain security and invite developer participation, as NIAP has done with Common Criteria Protection Profiles, which may provide it more influence over the standards and certification regime. However, this path is likely to require more time and engender less developer acceptance than participating in industry-driven consensus standards efforts and adopting their products. Experience indicates that industry often responds with greater agility to emerging threats than do government agencies or regulators.

**Approaching Acquisition Differently**

**RECOMMENDATION 15**

**DASD(SE)** direct JFAC to issue guidance that establishes product and supply chain assurance standards for government acquisition of COTS and OSS products.

---



## Chapter 4: Supporting Lifecycle Operations

### 4.1 PROGRAM PROTECTION PLANNING FOR FIELDIED SYSTEMS

#### TRANSITION OF PPPS FROM ACQUISITION TO SUSTAINMENT

The requirement to include cyber supply chain in the PPP was first introduced in 2011 along with the expansion to it being a mandatory document at all acquisition review milestones, as shown in Figure 6. The initial guidance in the Defense Acquisition Guidebook recognized the need for continuation of program protection planning into the sustainment phase, but deferred development of a process for handoff of the plan and updates beyond acquisition.<sup>65</sup>

With the approval of 76 Acquisition Category 1D/1AM PPPs across all of the acquisition phases, the Department has recognized the need to ensure that responsibilities for the program manager are clearly assigned to continue protection of critical information, technology and components, and to ensure that PPPs are updated throughout the lifecycle.<sup>66</sup> Army and Air Force have issued guidance assigning responsibilities for PPP preparation, implementation and maintenance, starting in acquisition and continuing through the lifecycle.<sup>67, 68</sup> The enclosure on “Cybersecurity in the Defense Acquisition System” will require that, after the full rate production or full deployment decision, the PPP will transition to the PM responsible for system sustainment and disposal.<sup>69</sup>

These documents focus primarily on comprehensive PPP development during the acquisition phase and updating those PPPs during the operations and support phase. Implementation of the plans during acquisition is largely within the control of the PM, under the oversight of the appropriate Service Acquisition Executive (SAE). Upon transition to sustainment, however, PPP implementation falls to the various supply, maintenance, and transportation organizations in the Military Services and Defense Logistics Agency (DLA) that do not report to the PM.

In some sustainment areas, existing processes and information systems are well equipped to act upon program protections. For example, protecting program information, both classified and controlled unclassified information, is built into current sustainment processes and systems so long as the information is properly marked when delivered by the PM. In other areas, this is not the case. For example, supply chain management disciplines applied during acquisition are not automatically carried forward into DoD spare parts procurement practices. Those practices routinely replace original suppliers through spare parts competition, use substitute items when the original is no longer available,

---

65. Defense Acquisition University, *Defense Acquisition Guidebook*, “Chapter 13 – Program Protection,” Section 13.10.4. Available at: <https://acc.dau.mil/CommunityBrowser.aspx?id=492081#13.10.4> (Accessed November 2016.)

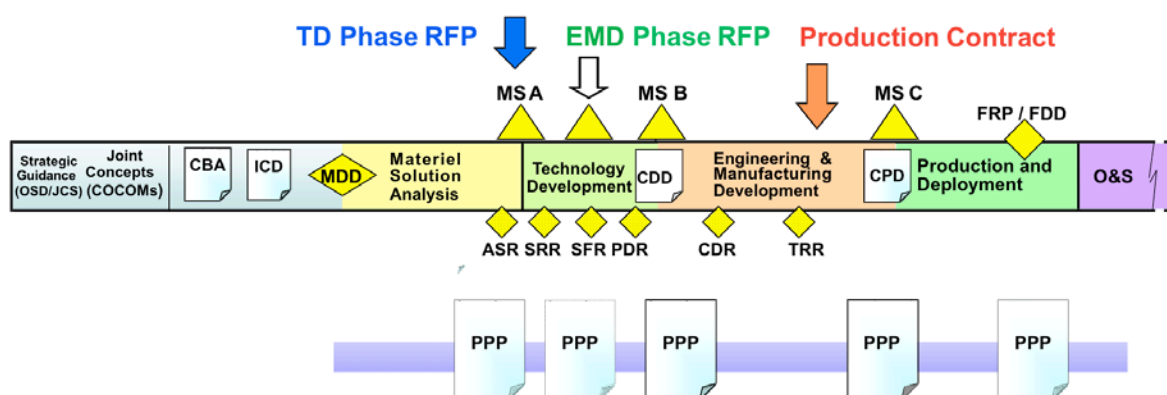
66. See acquisition category information at: <https://dap.dau.mil/glossary/pages/1382.aspx> (Accessed December 2016.)

67. Department of the Army, *Army Regulation 70–77*, “Program Protection” [April 2014].

68. Secretary of the Air Force, *Air Force Pamphlet 63-113*, “Program Protection Planning for Life Cycle Management,” [2013].

69. USD(AT&L), *Cybersecurity in the Defense Acquisition System*, DoDI 5000.02, [January 26, 2017], Enclosure 14, pg. 170.

## Supporting Lifecycle Operations



**Figure 6:** Program protection activities can inform solicitations.

and manage items at the part number level with limited visibility of weapons system applications. Consequently, the emphasis on trusted suppliers and parts provenance established in the PPP may be part of the PM's plan for the lifecycle, but may be lost in translation for parts managed by the DoD supply system.

Maintenance and repair activities are also part of the cyber-attack surface and need to implement the protections identified in the PPP. With the exception of maintenance contracts under the direct purview of the PM, these activities also depend on practices, systems, and reporting chains that the PM does not control.

Component-level repair and component-level parts procurement often cut across weapons system applications. Because the supply system values interchangeability and the ability to move inventories where needed, components that are critical in one application may need to be managed as critical for all. Current policy (DoDI 5200.39) recognizes this need for horizontal protection of CPI, and assigns responsibility to USD(AT&L) who coordinates with the Military Services to ensure CPI information is entered in the Acquisition Security Data Base (ASDB).<sup>70</sup> The DoD horizontal protection database provides online storage, retrieval, and tracking of CPI and supporting program protection documents to facilitate comparative analysis of defense systems' technology and align CPI protection activities across the DoD. When it comes to maintenance and parts procurement, however, the sustainment systems of the Military Services are not driven by the ASDB.

In cases where supply chain or parts problems have been identified for fielded systems, DoD parts information systems lack the ability to easily identify the affected weapons systems and to inform PMs to take appropriate mitigating actions. This is a long-standing issue in dealing with parts obsolescence issues and counterfeit parts. The PM usually does not have a bill of materials for the system that goes all

70. USD(I)/USD(AT&L). "Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)," DoDI 5200.39.

## Supporting Lifecycle Operations

the way to the bottom of the supply chain, and hence has to launch an inquiry to determine whether the weapons system is affected. Even if PMs had a complete bill of materials for their weapons systems, DoD lacks a data system that can invert the list and identify all the weapons systems that use a particular part. This obstacle impedes horizontal protection in dealing with parts vulnerabilities as they are reported, and is a major factor in limiting DoD's ability to recover from a cyber supply chain attack and restoring weapons systems to a trusted state. One best practice in this area is the Army's Multifunctional Obsolescence Resolution Environment (MORE) system, which has over 250,000 parts mapped to higher level assemblies and weapons systems applications.<sup>71</sup> Although developed for parts obsolescence problems, this type of system could evolve to be a significant DoD-wide tool for recovery from and response to exploitation of parts vulnerabilities.

PMs can ensure PPP implementation during acquisition, but Military Service Systems Commands and DLA need to take responsibility for item-level protection during sustainment.

### FIELDed SYSTEMS

Weapons systems fielded prior to the advent of PPPs make up the overwhelming majority of support for the Department's total warfighting capability, and will do so for years to come. Frontline weapons systems such as *Patriot*, *AEgis*, and *AMRAAM* are cases in point. During the years that these systems have been in the field, potential adversaries have had ample opportunities to learn about critical components and supply chains, identify latent vulnerabilities, and evaluate future cyber-attack possibilities. As referenced earlier, Cyber Awakening exercises have demonstrated that exploitable vulnerabilities exist and that the potential effects on warfighting capability are serious.

For such systems, critical components have not been identified and original suppliers were not subject to the vetting now required. While known vulnerabilities continue to exist, new vulnerabilities continue to be discovered with no formal process for mitigation. The protections defined in PPPs for new systems are urgently needed for important fielded systems. Without PPPs for fielded weapons systems, U.S. military capability readiness is uncertain.

### RECOMMENDATION 16

**USD(AT&L), in coordination with the Military Service Chiefs,** require development of a sustainment Program Protection Plan for designated fielded systems.

---

Congress has expressed similar concerns. Section 1647 of the FY 2016 NDAA on "Evaluation of cyber vulnerabilities of major weapons systems of the Department of Defense" requires that major systems be

---

71. U.S. Army Aviation and Missile Research, Development, and Engineering Center (AMRDEC), "Success Stories – The MORE Tool." Available at: <https://www.amrdec.army.mil/amrdec/success-more.html> (Accessed November 2016.)

---

## Supporting Lifecycle Operations

prioritized by the Chairman of the Joint Chiefs of Staff (CJCS) for evaluation and that cyber risks be mitigated.<sup>72</sup>

Designation of high priority fielded systems for sustainment PPPs should be consistent with the DoD response to related Congressional requirements. The guidance developed by ASD(L&MR) and DASD(SE) should explicitly address:

- Elements of the acquisition phase PPP analysis that need to be completed for fielded systems in the sustainment PPP;
- Relationship to the Life Cycle Sustainment Plan (LCSP);
- Responsibility for periodic reviews of the Sustainment PPP and implementation throughout the lifecycle;
- Responsibilities of Military Service Materiel or Systems Commands and Defense Agencies in implementing program protection within sustainment processes and information systems;
- Horizontal protection responsibilities and enabling capabilities; and
- Capabilities for recovery from an attack that exploits supply chain vulnerabilities, including visibility of affected parts and the weapons systems, so that weapons systems can be restored to a trusted state.

### RECOMMENDATION 17

**ASD(L&MR) and DASD(SE)** develop and promulgate guidance for the content of the sustainment Program Protection Plan and the implementation in sustainment processes.

---

## 4.2 COLLECT AND ACT ON PARTS VULNERABILITIES

As examined in this report, electronic parts and systems are vulnerable to physical, cyber, and cyber-physical threats. The Department has made some progress (through recent regulatory actions) to improve its awareness when DoD contractors discover a confirmed or suspected counterfeit electronic part as well as when contractors experience a cyber-attack on an information systems that exposes DoD information to loss of confidentiality. No DoD system currently collects event information on cyber-physical attacks of electronic components as its primary function. This might be represented by the insertion or corruption of the firmware or software that governs the functionality of such parts and the operation of systems that employ such parts. DoD's situational awareness of cyber supply chain threats is currently limited as contractors are not required or even encouraged to make voluntary reports on cyber-physical attacks on electronic parts. Even if such information were collected, the Department

---

72. *NDAA for Fiscal Year 2016*, Public Law 114-92 [November 2015], Section 1647.

### Supporting Lifecycle Operations

lacks the means to rapidly respond to cyber-physical events that, notionally, should encompass as distinct capabilities categorization, assessment, notification, reaction, and response to reported events.

Cyber-physical attacks may not become known for some time after the attack was executed. Once evidence of the event is detected, it is crucial to act quickly to limit the spread of the attack and otherwise mitigate its consequences. Contractors are afforded 72 hours to report to the DoD Cyber Crime Center (DC3) with respect to cyber-attacks covered by the “Safeguarding Covered Defense Information and Cyber Incident Reporting” DFARS. The present regulations concerning counterfeit parts are relatively lenient and expect reporting within 60 days of when the contractor becomes aware.<sup>73</sup> There are many indicators that defense industrial base contractors have been slow to report counterfeits and in some cases have sought to avoid the responsibility altogether. Deficiencies in reporting work against the ability of the DoD community to share information on threats, vulnerabilities, attacks, consequences and response. In a crisis or wartime situation, such delays could have very adverse effects upon force readiness and function.

Logistics plays a crucial role in DoD’s ability to sustain deployed equipment. In the commercial world, “best-in-class” logistics systems are highly integrated and employ advanced automation methods—using advanced methods of data collection and analytics to identify, respond to, and recover from adverse supply chain events. DoD should seek to better understand the strategies and methodologies of commercial companies in data-driven supply chain risk management. Many of these techniques can reduce vulnerability to attacks mounted through weak links in the supply chain and limit harm should an attack nonetheless occur. The Department currently lacks the parts visibility to the bottom of the supply chain and does not have access to “gold standard” parts or the data needed for analysis of discovered vulnerabilities and successful attacks. A systematic method is needed to identify and authenticate a gold standard of key electronic parts. There is no consistent or assured means to authenticate provenance or pedigree of parts currently in production by reference to embedded authentication or traceability information.

---

73. In contrast, newly released guidelines from DHS, effective Apr. 1, 2017, require federal civilian agencies to report cyber incidents, including those which affect supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS), within one (1) hour of detection. Reporting by entities other than Federal Executive Branch civilian agencies is voluntary. US-CERT Federal Incident Notification Guidelines are available at: <https://www.us-cert.gov/incident-notification-guidelines> (Accessed December 2016.)

---

**Supporting Lifecycle Operations**

---

**RECOMMENDATION 18**

**USD(AT&L)** direct programs to acquire a gold standard to test reference parts; and acquire hardware and software data rights for use in diagnosing malicious tampering:

- Contract clauses should be made available to program offices so that, selectively, for systems at high risk or of high impact, they may establish a contractual right, if exercised, to require the cooperation of the parts supplier in the evaluation of suspect parts against original and authentic materiel.
  - The DoD Office of General Counsel (OGC) should be consulted on methods to assure contractors that DoD will protect the security and proprietary character of reference parts and source data.
- 

**RECOMMENDATION 19**

**ASD(L&MR)** commission a feasibility study to demonstrate visibility to the bottom of the supply chain for critical parts; also to capture this information and include it in a DoD parts application database:

- The study should distinguish between systems now in sustainment versus those presently being manufactured or in design or development. The methods and outcome of such efforts may vary among these categories, along with the vulnerability to attack.
  - The study should assess the present practices of DoD contractors to collect and retain the “as-built” configuration of key systems.
  - The study should examine what can be accomplished by DoD Components and support contractors to extend the parts application database past into operational and sustainment phases.
  - The study should report on costs and benefit both to contractors and to DoD Components.
- 

Critical weapons systems are vulnerable to supply chain attacks. This risk is especially acute as concerning systems that continue to rely upon electronic parts that are out of production, obsolescent, or otherwise unavailable from trusted sources. Many systems in DoD’s inventory, upon which the nation will rely for years to come, are in this category of exposure. DoD presently receives, through GIDEP, at least some information on counterfeit electronics (which could harbor malicious code or unintended functionality) and, at least in theory, it could receive reports of cyber-attacks on hardware through the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Mitigation of known or suspected supply chain attacks requires timely and effective communication of event information to the operators of systems that are similarly at risk. Today, the Department generally does not know what electronic parts are installed or deployed in equipment that is at risk. DoD has only limited ability to

### Supporting Lifecycle Operations

rapidly identify and assess suspected hardware or software attacks upon electronic parts, though JFAC will assist with this function. Upon discovery of an attack, the ability to find similar equipment will be time-sensitive. However, DoD is presently very limited in its ability to communicate what it learns of reported attacks on electronic parts to users of equipment with the same parts. This information deficiency will slow the ability of the Department to warn operators, stop the spread of attacks, and implement timely measures of response and recovery.

As DoD evaluates how to modernize its logistics operation, it should assess and evaluate both commercially derived and custom solutions that will employ large-scale collection of supply chain information, utilize data analytics to anticipate supply chain risk and act upon adverse events, and to automate targeted notification of exposed or compromised parts. DoD should coordinate with other federal agencies, US-CERT, ICS-CERT, Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), and corresponding international organizations to improve the collection of information on known or suspected cyber-physical attacks, expedite notification and accelerate assessment and recommendation of responsive and corrective measures.

Effective response to supply chain attacks requires collection of event information, as well as analysis of reported data to determine its functional impact. One of the obstacles to protection of the electronic part supply chain against attack has been the absence of standards and methods to evaluate software and firmware and determine whether there has been tampering or insertion of malicious code. The Department cannot be assured that it is informed of the identity of all sources of electronic parts that may work their way into the supply chain. A shared vulnerability database of installed hardware is needed to promulgate corrective actions across weapons systems.

#### RECOMMENDATION 20

**DASD(SE)** should direct JFAC to:

- Develop a vulnerability database fed by multiple sources (e.g., DoD programs, commercial databases, DIA, contractor reports, Hardware CERT analyses).
  - Use data analytics to support detection and characterization of nefarious activity.
  - Incorporate monitoring input and intelligence received from JAPEC regarding exfiltrated design data.
-

## Chapter 5: Pursuing Technical Solutions

DoD systems currently require microcircuits that have known provenance. At one time this was accomplished by designing and fabricating ASICs for DoD needs. The time to design and test a new design has increased in recent complementary metal oxide semiconductor (CMOS) nodes and the costs have grown significantly. Nonetheless, DoD continues to have a need for custom state-of-the-art components to meet requirements for high-performance and low-power consumption.

### 5.1 CUSTOM FABRICATION OF STATE-OF-THE-ART MICROELECTRONICS

Microelectronics owes much of its development to the DoD. Through the 1970s and 1980s, DoD research investments laid the foundation for the generations of bipolar and CMOS devices that were initially applied to military systems and then applied with great success to the commercial marketplace. The situation began to change in the 1990s with the growing scale of investment, making it difficult for small volume fabricators to keep pace with the latest innovations in lithography and device fabrication. Increasingly, only the large scale commercial fabricators had the capital available to make the research and development precursors of future generations of CMOS nodes. Beyond the 90nm node, the \$3 billion to \$5 billion capital expense of semiconductor fabrication plants (fabs) caused commercial volumes to drive semiconductor factory investment, thus making the building of a stand-alone fab for DoD needs increasingly unfeasible. A Trusted Foundry program is an arrangement with an existing commercial semiconductor factory to utilize the commercial process to fabricate chips that have specialized designs for DoD.

Through the Trusted Foundry program, the Department gains the advantages of scale that commercial fabricators enjoy while maintaining unique designs. A state-of-the-art fabricator must initiate processing on 500 wafers per day to maintain process stability, as the performance data from wafers is used to tune the processing conditions to ensure device performance. The majority of these wafers go to commercial applications, while the much smaller number of DoD wafers benefit from the cost sharing with the commercial parts. The fabrication cost per wafer is several thousand dollars, costing about \$1 billion to operate the fab per year. Adding a new node to a fab incurs significant new capital expense. A Trusted Foundry program permits DoD to avoid these costs by co-fabricating with the commercial fab.

#### RECOMMENDATION 21

**The Secretary of Defense** pursue a relationship with a commercial state-of-the-art foundry, without investing in a DoD-owned state-of-the-art foundry.



---

**Pursuing Technical Solutions****5.2 SPLIT FABRICATION AND OTHER ALTERNATIVES**

Much of the capital expense of a state-of-the-art fab is related to the transistor fabrication because the wiring layers use relatively few new tools. Split fabrication uses the concept of building the transistors in one factory and then moving the wafers to a different factory where the wiring layers are built. In this way the transistor fabricator does not have insight into the use of individual transistors and is less able to know how a fabrication change would affect the final chip. The fab where the wiring layers are done can infer much of the way in which the chip will be used and must have a high level of trust. However, this is more easily obtained and maintained due to the lower capital cost of the wiring level steps.

The fabrication process needs to address both malicious insertion and design exfiltration, but commercial fabrication processes present challenges for the Department. The fabrication of masks and wafers is so challenging at state-of-the-art feature size that malicious manipulation of features is unlikely, even for a sophisticated adversary. Consequently, risk may be low enough to be acceptable even in offshore facilities. By contrast, design exfiltration is a substantial risk that will need long-term mitigation through technical means (e.g., anti-tamper, obfuscation, or split-fab) in order to use commercial state-of-the-art facilities. Similarly, long-term planning for the logistical phase of a chip lifecycle needs to protect against an attacker degrading or altering the die or its packaging, or substituting a malicious or counterfeit part, with provenance tracking to ensure parts used in critical applications are of low risk.

Therefore, DoD should use the time provided by the current Trusted Foundry contract to develop long-term options for access to state-of-the-art commercial foundry capabilities that do not rely exclusively on trust. DASD(SE) should determine in what circumstances the risk of malicious insertion in state-of-the-art ASICs in commercial fabrication is low enough to be accepted. The Assistant Secretary of Defense for Research and Engineering (ASD(R&E)) should expand efforts to validate and transition technologies from DARPA and elsewhere for protecting design exfiltration during fabrication. Split fabrication options provide great promise as a way to utilize foundries with state-of-the-art front-end processes that are not entirely trusted. Research is needed to provide methods to prevent tampering and to allow unique identification of a die in downstream logistics processes.

**RECOMMENDATION 22**

**Defense Advanced Research Projects Agency (DARPA) and Intelligence Advanced Research Projects Activity (IARPA)** continue R&D efforts to demonstrate a fully capable solution for split fabrication.

---

**DESIGN TOOL CHAIN**

A Trusted Foundry program ensures the provenance of the fabrication process, thereby providing a partial solution to assuring total provenance. However, it does not mean that the design files or the

### **Pursuing Technical Solutions**

masks have not been tampered before entering the fab. DoD needs assurance that upstream processes, including design libraries, computer aided design (CAD) tools and simulators, and mask design and fabrication, are free from malicious tampering.

#### **RECOMMENDATION 23**

**DASD(SE)** issue guidance to ensure the integrity of the design tool chain.

---

#### **FIELD PROGRAMMABLE GATE ARRAYS**

Field programmable gate arrays (FPGAs) are widely used in recent DoD systems. The ability to determine the chip logical function using a programming language means that the engineering team can have rapid design and test cycles. It also allows for future patching of a fielded system.

FPGAs have downsides as well. The commercial industry produces new devices each year that increase function and ceases manufacturing older devices. Finding replacement parts for an older system is quite difficult. Some vendors produce parts with DoD needs in mind which consequently provides longer availability or one time buy options. Additionally, a device whose logic can be reprogrammed also represents system vulnerability if an adversary can gain access to the programming port.

#### **RECOMMENDATION 24**

**USD(AT&L)** contract with FPGA vendors who have assured parts for DoD use.

---

#### **OBSOLETE PARTS**

Many DoD systems contain microelectronic parts that are no longer in production with the same specifications as the parts used to fabricate the system. Currently, DoD mitigates this risk by fabricating key legacy parts using DMEA and by purchasing parts.

The required performance of many of these parts is significantly below state-of-the-art parts. This provides DoD with additional options: replicate the function of the original part using an FPGA, emulate the part using a processor, or emulate the performance of the entire board with one or more parts. This provides a route for DoD to also mitigate vulnerabilities that have been discovered in the existing system. Beneficial functionality can be added to the FPGA, processor, or board to ensure that the vulnerability cannot be exploited.

**Pursuing Technical Solutions**

**RECOMMENDATION 25**

**Defense Microelectronics Activity (DMEA)** continue to provide non-state-of-the-art parts that cannot be obtained commercially without compromising mission performance that also integrate transparently with existing hardware and software.

---

### **5.3 ADDITIONAL RESEARCH**

Supply chain security for a microelectronic subsystem is an assurance matter. Cybersecurity professionals generally seek confidence that attackers cannot compromise the subsystem's operation by altering its design, its components, or the final full assembly. Supply chain attacks might target a microelectronic subsystem's building blocks, the processes involved in producing or combining those building blocks, or the entire assembly before it is built, while it is being built, or after it has been deployed. So defenses must protect against efforts to compromise artifacts (i.e., components, boards, racks, etc.) and protect against efforts to compromise processes (i.e., design, manufacturing, warehousing, shipping, installation, maintenance, etc.) While the Department has made progress in developing some of the needed defenses, more research could help provide new tools to better understand and expand on existing defenses to address cyber supply chain security.

Supply Chain Security is a research area that needs continued investment and development of a research community that can advance both basic and applied research that addresses not only commercial needs but also national security needs, where the bar is set higher. A framework is provided in Appendix A that can serve as a basis for planning further R&D investment programs.

---

**Summary**

## Chapter 6: Summary

The DoD cyber landscape has changed over the past few decades. The Department is now only a small fraction of the total global market for microelectronics, and the global supply chain is more non-linear than in prior years. This has promulgated complex interactions between suppliers, thus making it difficult for the Department to assure the parts placed into DoD weapons systems. Such changes impose new challenges which have increased the risk of cyber supply chain attacks during both the acquisition and sustainment phases. While current DoD program protection practices emphasize trusted suppliers in the acquisition phase, the task force found that systems fielded with no malicious insertions and no “known” inherent vulnerabilities are still subject to malicious insertion during sustainment.

Many DoD weapons systems were designed and manufactured before DoD had the opportunity to carry out the requisite testing and supply chain protection activities for needed parts. Cyber-active components have broad effects that can change the functionality in a weapons system. Such systems are complex and difficult to test. Better automated monitoring and detection techniques are needed to mitigate these risks. Modifications after fielding, including some intended to improve performance, monitor the system, or detect malicious actions may, in fact, expand the attack surface. Lifecycle Program Protection Plans must address this concern. The task force found that Cyber Awakening exercises have proven useful in identifying potential attack vectors and promoting subsequent mitigations in DoD weapons systems.

The evaluation of the current program protection process, as well as other practices to detect and assess potential vulnerabilities in hardware and software, offer insight in to how the Department can approach acquisition processes to remediate potential cyber-attacks in DoD weapons systems. The Joint Federated Assurance Center and the Joint Acquisition Protection and Exploitation Cell offer opportunities to monitor the cybersecurity landscape on an ongoing basis and report new trends in attacker techniques to access critical systems. The JFAC can also provide much needed expertise to program managers in support of lifecycle program protection planning and systems security engineering.

COTS vulnerabilities have been reported and can have significant impact on the security of DoD systems that incorporate affected products or components. Advanced adversaries can exploit their influence over COTS and OSS software to sabotage equipment, insert malicious code, or otherwise subvert the functionality and trustworthiness of military equipment. To address these concerns, a shared vulnerability database and a parts application database of installed hardware are needed to promulgate corrective actions across weapons systems.

The task force found that the capital cost of a DoD-owned, standalone, state-of-the-art semiconductor fabrication plant is not a feasible expense. Instead of investing in a new trusted foundry, DoD should use the remaining time in the current Trusted Foundry program to develop a long-term strategy for access to state-of-the-art commercial foundry capabilities that does not rely exclusively on trust. The task force recommends that DoD continue R&D investments by DARPA and other agencies for such a technology-enabled strategy. Split fabrication options should continue to be explored as a way to

## Summary

utilize foundries with state-of-the-art front-end processes that are not entirely trusted. Research should be continued in ways to prevent tampering and to allow unique identification of a die in downstream logistics processes. Where state-of-the-art performance is not required, preferential use of FPGAs from trusted sources should be pursued. Fostering new tools to better defend against cyber supply chain attacks should be an R&D priority for the next several years.

The task force recommends that USD(AT&L) strengthen lifecycle protection policies, enterprise implementation support, and R&D programs to ensure that DoD weapons systems are designed, fielded, and sustained in a way that reduces the likelihood and consequences of cyber supply chain attacks.

Table 2: Summary of Recommendations		Page
<b>Understanding Supply Chain Risk</b>		
1.	<p>Military Service Chiefs, with Military Deputies of SAEs, conduct at least one Cyber Awakening exercise per year and use the results of these assessments, in timely training of acquisition, operational, and sustainment personnel:</p> <ul style="list-style-type: none"> <li>• The training should be frequently updated as new exercises are conducted.</li> <li>• In-person training should be provided at the appropriate classification level for all affected personnel.</li> </ul>	11
<b>Mitigating Potential Vulnerabilities</b>		
2.	<p>USD(AT&amp;L) direct (DASD(Research) and DARPA to establish technical methods to identify discrepancies in software and firmware and for screening against malicious code or other hardware taints. This program should address:</p> <ul style="list-style-type: none"> <li>• Continuous monitoring of critical systems and affordable sensors backed by advanced analytics.</li> <li>• Technical approaches to obtaining trustworthy microelectronics from untrusted suppliers.</li> <li>• Examination of various methods of tagging, monitoring, and authentication of integrated circuits.</li> </ul>	18
3.	USD(AT&L) work to promulgate new regulations to eliminate the disincentives for industry self-reporting of counterfeits.	18
4.	<p>USD(AT&amp;L) direct the Defense Standardization program office to modernize the GIDEP reporting system and extend GIDEP to provide information to the JFAC:</p> <ul style="list-style-type: none"> <li>• Enhance GIDEP's functionality, funding, and staffing to include enhanced capability to rapidly communicate on vulnerability, events, and mitigation to users of parts that are under attack or at risk.</li> <li>• Expand GIDEP's charter to encompass reports of software and firmware attack as well as hardware.</li> <li>• GIDEP should inform JFAC of counterfeit components by automated means.</li> </ul>	19
<b>Approaching Acquisition Differently</b>		
5.	<p>USD(AT&amp;L) ensure that DoDI 5000.02 makes secure design and realistic risk assessment a core element of PPPs:</p> <ul style="list-style-type: none"> <li>• Each program manager should develop a rigorous security model (naming potential attacks) for weapons systems during specification with mandatory analysis of efficacy verifying that design and implementation will meet security requirements with high assurance.</li> <li>• Each program manager should incorporate funded in-depth security review of critical systems at key points pre-initial operational capability and during operations with the aims of remediating security flaws and improving acquisition, engineering, operational, or sustainment security. Such reviews should be conducted by a specialized organization or organizations to be established in or endorsed by JFAC.</li> </ul>	22

## Task Force on Cyber Supply Chain

### Summary

6.	<p>USD(AT&amp;L) ensure that DoDI 5000.02 anticipates the need for resilience, ongoing evaluation, and upgrade:</p> <ul style="list-style-type: none"> <li>Each program manager should specify design elements supporting resiliency including well defined interfaces for encapsulated subsystem allowing substitution of alternate or newly hardened implementations as well as procedures and testing to ensure the viability of substitution and upgrade.</li> <li>Each program manager should establish design elements and processes to identify and replace parts or subsystems with known or recently discovered vulnerabilities.</li> </ul>	22
7.	<p>USD(AT&amp;L) promote PPPs that encompass cradle to grave protection for new and existing systems:</p> <ul style="list-style-type: none"> <li>ASD(L&amp;MR) should revise the Logistics Assessment Guide to include program protection as one of the areas to be reviewed periodically after IOC.</li> <li>Each PPP should be transitioned to the program manager responsible for sustainment and disposal.</li> </ul>	23
8.	<p>USD(AT&amp;L) explore avenues to improve training and standards:</p> <ul style="list-style-type: none"> <li>DASD(SE) should set standards for criticality that are appropriate for mission assurance.</li> <li>PMs responsible for PPPs should complete training prior to taking command.</li> </ul>	24
9.	DIA coordinate with JAPEC to focus its resources on specific targeted, adversarial collection activities.	26
10.	USD(I) enhance current DIA supplier vetting by contracting for commercial due diligence.	27
11.	<p>Deputy Secretary of Defense update the JFAC charter to:</p> <ul style="list-style-type: none"> <li>Establish JFAC as a DoD-wide hardware and software assurance organization with a mandate to support Program Management Offices, Program Executive Offices, and sustainment activities.</li> <li>Develop prescriptive standards and requirements for hardware and software assurance processes and tools.</li> <li>Provide the program manager and the JFAC Steering Committee with an independent perspective on risk articulated by a peer-level official in JFAC in cases where a program is unable to adhere to standards or requirements.</li> </ul>	29
12.	<p>USD(AT&amp;L) and USD(I) charter, fund, and staff JAPEC to:</p> <ul style="list-style-type: none"> <li>Coordinate intelligence collection requirements for acquisition programs</li> <li>Coordinate and provide briefings of specific threat activities to targeted programs</li> </ul>	30
13.	USD(AT&L) issue guidance to programs to work with JFAC and ensure adequate funding and authority for the JFAC mission.	32
14.	USD(AT&L) direct the establishment of a Hardware CERT to track the reporting and remediation of vulnerabilities in COTS hardware and embedded firmware.	35
15.	DASD(SE) direct JFAC to issue guidance that establishes product and supply chain assurance standards for government acquisition of COTS and OSS products.	36
<b>Supporting Lifecycle Operations</b>		
16.	USD(AT&L), in coordination with the Military Service Chiefs, require development of a sustainment Program Protection Plan for designated fielded systems.	39
17.	ASD(L&MR) and DASD(SE) develop and promulgate guidance for the content of the sustainment Program Protection Plan and the implementation in sustainment processes.	40
18.	<p>USD(AT&amp;L) direct programs to acquire a gold standard to test reference parts; and acquire hardware and software data rights for use in diagnosing malicious tampering:</p> <ul style="list-style-type: none"> <li>Contract clauses should be made available to program offices so that, selectively, for systems at high risk or of high impact, they may establish a contractual right, if exercised, to require the cooperation of the parts supplier in the evaluation of suspect parts against original and authentic materiel.</li> <li>The DoD Office of General Counsel (OGC) should be consulted on methods to assure contractors that DoD will protect the security and proprietary character of reference parts and source data.</li> </ul>	42

Summary

19.	<p>ASD(L&amp;MR) commission a feasibility study to demonstrate visibility to the bottom of the supply chain for critical parts; also to capture this information and include it in a DoD parts application database:</p> <ul style="list-style-type: none"> <li>• The study should distinguish between systems now in sustainment versus those presently being manufactured or in design or development. The methods and outcome of such efforts may vary among these categories, along with the vulnerability to attack.</li> <li>• The study should assess the present practices of DoD contractors to collect and retain the “as-built” configuration of key systems.</li> <li>• The study should examine what can be accomplished by DoD Components and support contractors to extend the parts application database past into operational and sustainment phases.</li> <li>• The study should report on costs and benefit both to contractors and to DoD Components.</li> </ul>	42
20.	<p>DASD(SE) should direct JFAC to:</p> <ul style="list-style-type: none"> <li>• Develop a vulnerability database fed by multiple sources (, DoD programs, commercial databases, DIA, contractor reports, Hardware CERT analyses).</li> <li>• Use data analytics to support detection and characterization of nefarious activity.</li> <li>• Incorporate monitoring input and intelligence received from JAPEC regarding exfiltrated design data.</li> </ul>	43
<b>Pursuing Technical Solutions</b>		
21.	The Secretary of Defense pursue a relationship with a commercial state-of-the-art foundry, without investing in a DoD-owned state-of-the-art foundry.	44
22.	DARPA and IARPA continue R&D efforts to demonstrate a fully capable solution for split fabrication.	45
23.	DASD(SE) issue guidance to ensure the integrity of the design tool chain.	46
24.	USD(AT&L) contract with FPGA vendors who have assured parts for DoD use.	46
25.	DMEA continue to provide non-state-of-the-art parts that cannot be obtained commercially without compromising mission performance that also integrate transparently with existing hardware and software.	47

---

**Appendix A: Directions for Research to Assure Supply Chain Security**

# **Appendix A: Directions for Research to Assure Supply Chain Security**

## **APPROACHES TO ASSURANCE**

Processes to enhance assurance standards for the hardware and software of DoD systems will be aided by a careful consideration of how differing approaches to trust will affect the implementation of assurance standards. Viewed abstractly, assurance can be increased in an artifact or process “S” by relocating what is trusted—i.e., trust in “S” could be made to follow from trust in something else (say) “S’,” which is more trusted than “S.” For example, encapsulating a chip in a tamper-proof case promotes trust that the chip has not been altered only because the tamper-proof technology is trusted. The tamper-proof case increases assurance when there is concern with attacks that involves physical access to the chip before or after it has been installed. But a tamper-proof case does not defend against attacks that compromise the design or fabrication of the silicon wafer. If those are the attacks of concern, then there is little reason to have more trust in the encapsulated chip than in the original.

A collection of means will be needed to defend against the broad spectrum of possible supply chain attacks. Individual means might protect only some artifacts or processes involved in creating the microelectronics subsystem, but a collection of means could cover the subsystem for its full lifecycle: building blocks and design, then synthesis, followed by installation, maintenance, and ultimately decommissioning. The completeness of such a defense could be established by analyzing its coverage relative to the operator’s understanding of what attacks are likely or feasible, and to expectations about adversary capabilities. To strengthen this analysis of coverage, a worthy research goal is to:

1. Develop formal languages for rigorously describing the scope for a means of defense given some assumed attack classes and capabilities for attackers
2. Devise algorithms to perform automated analyses that determine coverage to the provided means (and report gaps that remain)

## **AXIOMATIC BASIS FOR ASSURANCE**

---

Means to establish assurance in an artifact or process will be axiomatic, analytic, synthetic, or some combination. An axiomatic basis for trust gives the weakest form of assurance. With this type of defense, an artifact or process is trusted based on beliefs that have been accepted on faith. Something might be trusted, for example, because it is sold by a given company. In this case, trust is relocated from the object to the company, thereby putting faith in the company’s actions being consistent with its reputation. Here, the basis for trust has nothing to do with the artifact itself or with the manner in which it was assembled, hence why this basis for trust provides a weak form of assurance.

In the scientific literature, a small number of assertions are enshrined as axioms when they are well understood and universally accepted because they have never been contradicted by experiment. It is far less compelling to put faith in a person’s nationality, a company, or any attribute that is not inherently coupled to guarantees about performance. Moreover, an axiomatic basis for trust cannot be dispositive



---

## Appendix A: Directions for Research to Assure Supply Chain Security

for any system that is too complex to understand completely—especially systems based on cutting-edge technology that have not been used in their intended environments.

### ANALYTIC BASIS FOR ASSURANCE

---

With an analytic basis for trust, testing or reasoning are used to justify conclusions about properties of interest. Trust in an artifact or process is being relocated to trust in some method of analysis. The feasibility of establishing an analytic basis depends on the amount of work involved in performing the analysis and on the soundness of any assumptions underlying that analysis.

- **Testing:** In theory, every input can be checked to conclude that some given property of interest will always be satisfied, but enumeration and checking of all possible inputs is not feasible for even a simple microelectronic subsystem because, typically, only a subset of the inputs would be checked. Thus, an assumption is being made that enough inputs are being checked to expose evidence of compromise. There is also an assumption that the evaluated attributes for each test are a sufficiently complete characterization of the subsystem's behavior to ensure confidence that said tests would reveal compromises.
- **Formal Verification:** Designs are often amenable to mathematical analysis, either by hand or automated in software. Such analysis is tantamount to proving a theorem about some model (e.g., a program or a circuit) so that it has sufficient fidelity to detect problems without losing them in translating to an abstraction. Today's state-of-the-art for such automated analysis:
  - a. Allows certain simple properties to be checked automatically for artifacts even if quite large.
  - b. Allows rich classes of properties to be verified by hand for (only) small artifacts.

Research in formal verification has steadily made progress on widening the class of properties that can be checked automatically, the size and complexity that can be handled, and the fidelity of models that are analyzed. This research should be continued. It is the foundation for enhancing the capabilities of automated analysis for detecting supply chain attacks (or many other types of attacks as well).

Analytic methods are most relevant when there is a model that spans all relevant uses and all interfaces to the environment. That is, the model must not ignore too many details. Complex systems, especially microelectronic systems with cyber-active components, hardly ever admit even the theoretical possibility of such a complete model. For example, when testing or analysis is focused on some set of interfaces, the assumption is that there are not additional interfaces. This assumption can be dangerous. By ignoring power usage and electromagnetic emissions (as well as other physical properties), for instance, other avenues of information leakage could also be ignored. This means that testing or analysis might determine that classified information cannot flow to an unclassified user, even though secrets actually can leak.

---

**Appendix A: Directions for Research to Assure Supply Chain Security**

---

**SYNTHETIC BASIS FOR ASSURANCE**

---

Finally, trust in an artifact or process can be ascertained because of its structure or how it was built. This is a synthetic basis for trust. Here, trust in the whole derives from trust in the way components that are being combined—a form of divide and conquer. For example, a synthetic basis for trust in artifact “A” of interest could require that:

1. The design ensures that the use of unaltered components yields an instance of “A” that behaves as intended.
2. Means are employed for the components to be trusted.
3. Every step in assembling, transporting, and operating “A” can be trusted.

Notice, (3) implies that if inputs to a step can be trusted, then the outputs from that step can be trusted as well. Also, the steps in (3) together must cover the entire lifetime of the system. So, for instance, transporting an artifact from one location to another during manufacture or even warehousing would be considered a step or part of a step.

When using a synthetic basis for trust, it pays to employ a method of composition that is linked to a procedure for establishing trust in the outputs of that method (assuming trust in the constituents). In fact, such linkages are a reason that employing a synthetic basis for relocating trust is so attractive. However, the full benefit of this synthetic trust requires that assurance be a consideration at every step of design and implementation, from the smallest components to final subsystem realization. Thus, more research is required to foster a “propagation of assurance” approach for the entire microelectronic subsystems found in today’s weapons systems.

**CREATING AND LEVERAGING INDEPENDENCE**

Replication is an especially important synthetic basis for trust. This structure combines  $2t+1$  replicas, ensures all receive a copy of each input, and votes on the replica outputs. Provided the replicas are independent—that is, a supply chain attack that affects the behavior of one replica will not have the same effect on another—then the replicated system will not be compromised and will remain available until  $t+1$  of the replicas have been compromised (which, by the independence assumption, requires  $t+1$  different supply chain attacks). But creating this  $t+1$ -fold increase in attacker work grows the system cost over  $2t+1$  fold.

Independence also is leveraged in split-fabrication approaches to building systems as mentioned earlier. Here, the system is assembled from separate partitions. These partitions are defined in such a way that a change to any subset causes easily detected misbehavior by the full system. By requiring the partitions to be independent, the attacker is forced to compromise the sources of multiple partitions in order to compromise the full system. This raises the cost of supply chain attacks. Split-fabrication is, today, feasible for certain (but not all) kinds of semiconductor packagings. Theoretical results about so-called “multi-party computations” offer the possibility that similar splitting could be used for software, though additional research is needed before the protocols will be practical. Whether the basic idea can be employed at the board level or above is an open question, requiring future research.

---

**Appendix A: Directions for Research to Assure Supply Chain Security**

Achieving independence is clearly quite important for defending against supply chain attacks. Blind buys, purchasing like components from separate producers, and contracting for diverse designs are all ways to develop the required independence. In addition, researchers have been investigating algorithms for creating artificial diversity. Such an algorithm, when given a single instance of a program or circuit description as input, will output a set of randomly perturbed but functionally equivalent instances. Elements of this set, by construction, perform the same task. Yet, the elements of the set will require different attacks to affect the same compromise, making these elements independent from each other with respect to supply chain attacks. Address space layout randomization (ASLR) in the Windows operating system is an example of such an algorithm. Further research should allow the Department to use the same general approach for creating independence in a broader range of systems (including FPGA descriptions and other regularly structured hardware substrates). In addition, further research can help understand the effects of combining different schemes for creating artificial diversity as well as how to compose subsystems that have been randomly perturbed in different ways.

**PUTTING IT TOGETHER**

Modern weapons systems have large numbers of microelectronic parts. A part may have millions of circuit elements, with complex interconnections. Also, some of the parts will be connected to sensors, and almost all of the parts will likely have thousands to millions of lines of programming (i.e., embedded firmware) that governs behavior. As a result, these microelectronic parts are too complex for comprehensive modeling. Moreover, the parts are often made by a global supply chain, with producers who may be unwilling to share design fabrication information in sufficient detail to enable analysis.

Consequently, the Department is limited primarily to axiomatic approaches for justifying trust in these lowest-level components, although sampling and extensive testing can be and are used to justify increased trust in component sources. Analytic and synthetic bases for trust remain available to manufacturers of weapons systems and to their subcontractors who are tasked with combining these lowest-level components. For example, the following collection of elements might be seen in a supply chain defense for the microelectronics assemblies found in weapons system.

1. Axiomatic basis: Purchase instances of each part from a large and diverse set of suppliers, thereby making it too costly for an adversary to perform supply chain attacks that, with a high degree of certainty, will affect all instances of a given part.
2. Synthetic basis: Employ tamper-proof packaging and unforgeable markings to prevent tampering with parts in transit.
3. Analytic basis: Record provenance (to identify who built, shipped, warehoused or otherwise handled a part or assembly) and assign trust according to judgments about the trustworthiness of those intermediaries.
4. Analytic basis: Employ sampling to collect measurements related to the operation of a system that to the user trusts, thereby establishing norms and use these norms to evaluate whether a given instance of the system can be trusted because it is equivalent to the instance measured.

---

**Appendix A: Directions for Research to Assure Supply Chain Security**

Each of elements (1) through (4) could potentially be more effective were it the starting point for some research. For (1), DoD is likely to use practical judgments such as shared ownership, common subcontractors, and geo-political connections when assessing whether two suppliers are diverse. Research might reveal better evaluation criteria (e.g., company structure, current customers and suppliers, financial state) for predicting likely independence of components from different suppliers. Continued research into tamper-proof packages and markings (element (2) above) is needed because of the co-evolution of attacks and defenses. Using provenance (element (3)) as a basis for trust clearly benefits from research in support of elements (1) and (4). And there has been, and continues to be, considerable research in testing (element (4)). This framework can also be found in the approach to “design for testability” where scan-chains or other maintenance interfaces are created for loading and accessing internal state, but with the focus on detecting benign faults. Other research in testing attempts to identify counterfeits. But the Department would benefit from funding testing approaches (perhaps supported by new design regimes that stipulate certain kinds of interfaces or decomposition) to determine if the internal logic has been altered to provide added function, perhaps in response to a triggering event.

**SUPPORT FOR SELF- VERSUS NON-SELF DETERMINATIONS**

By definition, support for reflection entails having an interface for learning a system’s state and its implementation. Reflection thus provides a way to characterize a system in terms of what it actually is, as compared to using some identifier for what the system is purported to be—i.e., “a book is not identified by its cover,” but rather identified by the sequence of characters it contains. Thus, it is important to have an interface available for reflection aids in detecting a compromised component because the interface exports information that can be compared against what is expected for an uncompromised component. Notice, for detecting a successful supply chain attack, it is not actually necessary to query specific parts of the state or implementation; it suffices to receive a summary that incorporates all the state and implementation details.

A cryptographic hash  $H(b)$  of a bit string “ $b$ ” is a relatively small value (e.g., 256 bits) that is likely to change in an unpredictable way if any of the bits in “ $b$ ” are changed. Cryptographic hashes thus implement for software or data the summary discussed above. So given a way to compute cryptographic hashes, some data or software (including firmware) can be checked for potential gaps. Such support is available today in COTS hardware, either as part of a standard processor (e.g., Intel’s® Software Guard Extensions (SGX)) or as a co-processor (e.g., the Trusted Computing Group’s Trusted Platform Module (TPM)). Few embedded computing systems take advantage of that functionality, though the research community has been exploring an embodiment (known as measured principals) for deploying the approach on personal computers and cloud servers. Further research investments will be necessary, both for the more prosaic aspects of running a system—software upgrades, system back-up, and day-to-day configuration changes (i.e., setting a new target location) bring new challenges—and also for understanding deployment issues on embedded computers.

Reflection capabilities for hardware are far behind what is possible for software. Scan-chains and other maintenance interfaces do provide visibility into some aspects of a system’s implementation and expected behaviors. Additional research could lead to architectures for achieving greater visibility

## **Appendix A: Directions for Research to Assure Supply Chain Security**

through these interfaces, making them effective for detecting symptoms of a supply chain attack. But because a program can always be written to simulate any given program, attackers in theory can create a compromised component that (until some trigger is activated) provides the same input and output functionality as an uncompromised component. Volkswagen's software for cheating pollution tests is an example of such a simulator.

Research advances in the following will make it harder for attackers to succeed, at least with post-deployment supply chain attacks:

- Non-digital operating attributes, such as timing, acoustic, thermal, or electromagnetic emissions, can allow a compromised component to be distinguished from a non-compromised one, even if both components seem to provide the same input and output functionality. Additional research is needed about how best to incorporate such measurements into an embedded system.
- Physically unclonable functions (PUFs) are circuits that evaluate some (unique) function that can be invoked by the chip hosting the circuit; the actual function computed depends on randomness found in hosting chip's silicon substrate. Alter the chip in any way and the functions implemented by its PUFs are likely to change. A PUF behaves like a hash function for a chip.
- Dielets present a method to verify the trustworthiness of a protected electronic component. A dielet would be inserted into the electronic component's package at the manufacturing site or affixed to existing trusted components, without altering the component's design or reliability. It could be queried at any time and would indicate if any tampering had occurred.
- Systems designed around subsystems that proactively perform periodic and automated self-testing and environment-testing are more resilient to post-deployment supply chain attacks. This is because multiple components of the subsystems would have to be altered in order to prevent the periodic testing from exposing a successful attack. Research would improve understanding of how best to build systems in this style.
- For larger assemblies, optical inspections can detect whether alterations have been made. The inside of a chip or a full circuit board could be inspected and this image could be compared with that of another image taken at an earlier time as a means to detect alterations.

**Appendix B: Cyber Awakening Exercises**

## **Appendix B: Cyber Awakening Exercises**

Contact the Defense Science Board office to access this appendix.

Appendix C: Joint Federated Assurance Center Charter

# Appendix C: Joint Federated Assurance Center Charter



DEPUTY SECRETARY OF DEFENSE  
1010 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1010

February 9, 2015

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS  
CHAIRMAN OF THE JOINT CHIEFS OF STAFF  
UNDER SECRETARIES OF DEFENSE  
DEPUTY CHIEF MANAGEMENT OFFICER  
COMMANDERS OF THE COMBATANT COMMANDS  
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION  
DIRECTOR, OPERATIONAL TEST AND EVALUATION  
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE  
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE  
ASSISTANT SECRETARIES OF DEFENSE  
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER  
ASSISTANTS TO THE SECRETARY OF DEFENSE  
DIRECTOR, NET ASSESSMENT  
DIRECTORS OF THE DEFENSE AGENCIES  
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Policy Memorandum (PM) 15-001 – Joint Federated Assurance Center  
(JFAC) Charter

EXPIRATION DATE: February 9, 2017

POINT OF CONTACT: For more information, contact the Office of the Deputy Assistant  
Secretary of Defense for Systems Engineering 571-372-6129

Section 937 of the National Defense Authorization Act for Fiscal Year 2014, Public Law 113-66, requires the Department of Defense to establish a joint federation of capabilities to support trusted defense system needs to ensure the security of software and hardware developed, acquired, maintained, and used by the Department.

Effective immediately, I am directing the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) to implement the attached Joint Federated Assurance Center (JFAC) Charter.

A handwritten signature in black ink, appearing to read "R. M. ...", is located below the text of the memorandum.

Attachment:  
As stated



## Appendix C: Joint Federated Assurance Center Charter

### Joint Federated Assurance Center Charter

1. **PURPOSE AND SCOPE.** This charter establishes and describes the Joint Federated Assurance Center (JFAC) mission, functions, construct, and responsibilities in accordance with the Department's Acquisition and Trusted Defense Systems strategy and policy.

2. **REFERENCES:**

- a. Public Law 113-66, National Defense Authorization Act for Fiscal Year 2014, section 937. Joint Federated Centers for Trusted Defense Systems for the Department of Defense
- b. Public Law 112-239, National Defense Authorization Act for Fiscal Year 2013, section 933. Improvements in Assurance of Computer Software Procured by the Department of Defense
- c. Public Law 111-383, Ike Skelton National Defense Authorization Act for Fiscal Year 2011, section 932, Strategy on Computer Software Assurance
- d. Public Law 110-417, Duncan Hunter National Defense Authorization Act for Fiscal Year 2011, section 254. Trusted Defense Systems
- e. Interim Department of Defense Instruction (DoDI) 5000.02, Operation of the Defense Acquisition System
- f. DoDI 5200.44, Protection of Mission and Critical Functions to Achieve Trusted Systems and Networks (TSN)
- g. NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations

3. **BACKGROUND.** Interim DoDI 5000.02, Operation of the Defense Acquisition System (reference e.), and DoDI 5200.44 (reference f.) define and implement the policy and strategy for TSN within the Department for covered programs. They require program offices to include software assurance (SwA) and hardware assurance (HwA) as part of program protection planning throughout the acquisition life cycle. Program offices and sustaining activities can leverage the JFAC to support the implementation of DoD SwA and HwA requirements.

4. **MISSION and OBJECTIVES.** The JFAC is the federation of all Department entities having software and hardware assurance capabilities needed by programs. The JFAC will develop, maintain, and offer software and hardware vulnerability detection, analysis, and remediation capabilities through a federation of internal, coordinated organizations and facilities from across the Military Departments, Defense Agencies, and other DoD organizations. The JFAC facilitates collaboration across Science and Technology (S&T), acquisition, Test and Evaluation (T&E), and sustainment efforts to ensure that SwA and HwA capabilities and investments are effectively planned, executed, and coordinated across the Department. The JFAC:



## Appendix C: Joint Federated Assurance Center Charter

- a. Supports program offices across the life cycle by identifying and facilitating access to Department SwA and HwA expertise and capabilities, policies, guidance, requirements, best practices, contracting, training, and testing support.
- b. Ensures requirements to innovate software vulnerability analysis, testing, and protection tools are provided to inform DoD R&D strategy development.
- c. Ensures requirements to innovate hardware vulnerability analysis, testing, and protection tools are provided to inform DoD R&D strategy development.
- d. Establishes and enables efficient and affordable acquisition and use of tools for SwA and HwA analysis and test.

### 5. JFAC FUNCTIONS. The JFAC:

- a. Identifies, promotes, and facilitates access to SwA and HwA capabilities in support of program offices, other DoD, and other Federal Government organizations throughout the acquisition life cycle, to include:
  - 1) Efforts to ensure an inventory of SwA and HwA resources, across DoD, including vulnerability analysis tools;
  - 2) Increasing awareness of vulnerability analysis tools, evidence-based practices, support environments, competencies, threats, and vulnerabilities; and
  - 3) Coordinating access to and capability for applying tools, evidence-based practices, support environments, and expertise across the Department.
- b. Acts as the DoD contact for interagency efforts for SwA and HwA policies, guidance, standards, acquisition practices, best practices, training, and testing support.
- c. Evaluates, over time, the impact of DoD investments and activities in support of SwA and HwA.
- d. Supports Department-level inquiries, studies, and reports regarding SwA and HwA.

### 6. JFAC MANAGEMENT CONSTRUCT:

- a. The JFAC comprises the existing supporting staff and elements selected by the participating DoD Component heads, or their designees, to collaboratively carry out JFAC activities to achieve the Steering Committee's strategies and objectives. Representatives from other Federal Government agencies may be invited to participate in the JFAC.
- b. The JFAC Steering Committee includes senior executive representatives from the following DoD Components:

## Appendix C: Joint Federated Assurance Center Charter

- 1) OUSD(AT&L)
  - 2) DoD CIO
  - 3) Department of the Army
  - 4) Department of the Navy
  - 5) Department of the Air Force
  - 6) Missile Defense Agency
  - 7) National Security Agency
  - 8) National Reconnaissance Office
  - 9) Defense Information Systems Agency
  - 10) Defense Microelectronics Activity
- c. The JFAC Working Group comprises, but is not limited to, the Steering Committee policy and technical representatives with responsibility to accomplish the Steering Committee's strategies and objectives. Additional members may be approved only by the Steering Committee.
7. RESPONSIBILITIES.
- a. USD(AT&L) shall:
- 1) Identify resource gaps, and strategies to mitigate them.
  - 2) Preside at all meetings of the JFAC Steering Committee and associated working groups, and provide administrative management of and support for the JFAC.
  - 3) Integrate JFAC SwA and HwA findings into DoD acquisition policy, guidance, and processes, as appropriate.
  - 4) Assure DoD R&D strategy is informed by SW and HW assurance capability needs.
- b. DoD CIO shall:
- 1) Invite comments from the JFAC when establishing standards and requirements for HwA and SwA to protect DoD information technology.
  - 2) Integrate JFAC findings regarding use of Department SwA and HwA capabilities into cybersecurity policies, guidance, controls, and practices.
  - 3) Collaborate with OUSD(AT&L) to ensure alignment between cybersecurity elements including policies, controls, guidance, and practices, and DoD acquisition elements including policy, guidance, and practices, for SwA and HwA.
- c. JFAC Steering Committee shall:
- 1) Develop the JFAC vision, goals, and objectives, provide oversight, and maintain accountability.
  - 2) Review and approve the JFAC concept of operations (CONOPS), as required.
  - 3) Review JFAC capability gap analysis and approve needed modifications.

**Appendix C: Joint Federated Assurance Center Charter**

d. JFAC Working Group shall:

- 1) Develop and update the JFAC CONOPS, as required.
- 2) Oversee operational execution of the JFAC.
- 3) Use JFAC performance and metrics to determine and report return-on-investment, as required.
- 4) Assess JFAC capabilities and capability gaps and recommend mitigations, as required.
- 5) Resolve conflicting policies, schedules, and priorities.

e. JFAC supporting staff shall:

- 1) Execute the JFAC CONOPS, which includes performing SwA and HwA tasks and conducting capacity gap analyses.
- 2) Support development of and updates to the JFAC CONOPS and JFAC operation, as required.
- 3) Recommend and supply metrics for JFAC performance and SwA and HwA.
- 4) Identify and maintain cognizance of JFAC operational capabilities and capability gaps, including resources needed to address the gaps, by priority.
- 5) Identify and analyze reported vulnerabilities in software and hardware, including systemic patterns of causation and mitigation approaches across DoD for covered programs, and other systems as appropriate, across the life cycle.
- 6) Monitor effectiveness of software tools and techniques, and provide data as required.
- 7) Interact with program offices in accordance with each DoD Component's communication plan.

f. Participating DoD Components shall:

- 1) Provide SwA and HwA capabilities and resources, and support for the JFAC and management construct.
- 2) Assist in the formulation of JFAC operational requirements.
- 3) Develop R&D budget requirements in coordination with the JFAC.
- 4) Nominate SwA and HwA capabilities and sustain inventory.
- 5) Develop a communication plan to manage interactions between the JFAC support staff, members and program offices.
- 6) Provide SwA and HwA capabilities to DoD programs and interact with program offices in accordance with each DoD Component's communication plan.
- 7) Execute the JFAC CONOPS based on direction and resources.

g. DMEA shall:

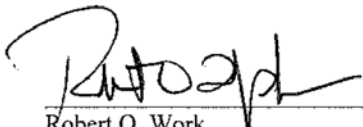
- 1) Coordinate with the office of the Deputy Assistant Secretary of Defense (Research and Development) (DASD(RD)) on requirements for the DoD R&D strategy to improve hardware vulnerability, testing, and protection tools.

**Appendix C: Joint Federated Assurance Center Charter**

h. NSA shall:

- 1) Coordinate with the Office of the DASD(RD) on requirements for the DoD R&D strategy to improve hardware and software vulnerability detection, analysis, testing, and protection tools, and
- 2) Support the JFAC Working Group with SwA and HwA subject matter expertise

This charter becomes effective upon signature and remains in effect until revised or rescinded.

  
Robert O. Work  
Deputy Secretary of Defense

9 February 2015  
Date

Terms of Reference

# Terms of Reference



ACQUISITION,  
TECHNOLOGY  
AND LOGISTICS

THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3010

NOV 12 2014

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board Task Force on Cyber Supply Chain

The defense industrial base consists of a set of cleared contractors and known performers. Capabilities developed, produced, and sustained by the defense industrial base are derived from known and, more importantly, unknown lower tier vendors and sub-suppliers that form a global supply chain supplying providing the necessary components and subcomponents. Globalization of technology introduces multiple opportunities to insert defects and malware into components in locations outside of US Government control which can eventually find their way into a defense system or to allow disruption of critical components at disadvantageous times.

The purpose of this study is to review the DoD supply chain risk management activities, including case reviews of specific acquisition program application and the resulting outcomes. The task force will assess whether current practices are able to effectively mitigate malicious supply chain risk, and whether opportunities exist to modify or strengthen practices to increase the effectiveness of current practices. Questions the task force will address include: Are the practices resulting in actionable risk mitigations that programs have implemented to reduce system vulnerabilities? Would there be benefit to a narrowed focus on a specific supply chain risk (i.e. microelectronics)? Can DoD practices be augmented with private sector actions? What can the industrial base do to improve supply chain management practices, and what commercial sector tools and practices might be brought to bear? Finally, since this is a cross-cutting threat that affects more than DoD, are there interagency activities that DoD could better leverage to reduce its risk?

I will sponsor the study. The Honorable Page Hooper and Dr. John Manferdelli will serve as Co-chairmen of the study. Ms. Melinda Reed, OUSD(AT&L), will serve as Executive Secretary. Lt Col Michael Harvey, USAF, will serve as the DSB Secretariat Representative.

The study will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act" and DoD Directive 5105.04, the DoD Federal Advisory Committee Management Program." It is not anticipated that this study will need to go into any "particular matters" within the meaning of title 18, United States Code, section 208, nor will it cause any member to be placed in the position of action as a procurement official.

A handwritten signature in black ink, appearing to read "Frank Kendall".

Frank Kendall

**Members of the Study**

## Members of the Study

### **Study Chairs**

Hon. Paul (Page) Hoyer	Onpoint Technologies Inc.
Dr. John Manfredelli	Google

### **Executive Secretary**

Ms. Melinda Reed	OUS(DAT&L)
------------------	------------

### **Members**

Dr. Mark Epstein	Qualcomm
Hon. Paul Kaminski	Technovation, Inc.
Mr. Steve Lipner	SAFECode
Dr. David Luzzi	Northeastern University
Dr. Michael McGrath	Private Consultant
Mr. Robert Metzger	Rogers Joseph O'Donnell, PC
Mr. Andrew Oak	Johns Hopkins University Applied Physics Laboratory
Dr. Fred Schneider	Cornell University
Dr. Robert Wisnieff	IBM

### **Defense Science Board**

Ms. Karen Saunders	Executive Director
CAPT Hugh "Mike" Flanagan	Deputy for Operations, Navy
CAPT Jeffrey Nowak	Deputy for Operations, Navy
Lt Col Victor Osweiler	Deputy for Operations, Air Force

### **Staff**

Mr. Marcus Hawkins	Strategic Analysis, Inc.
Dr. Toni Marechaux	Strategic Analysis, Inc.
Ms. Jeray Simms	Strategic Analysis, Inc.
Ms. Melissa Smittle	Strategic Analysis, Inc.

---

**Briefers to the Study**

## **Briefers to the Study**

### **April 23–24, 2015**

Mr. Scott Adams	SAF/AQX
Ms. Kristen Baldwin	OUS(D(AT&L))
Dr. William Chappell	DARPA
Mr. Chongkin Chin	Department of Defense
Ms. Joyce Corell	ODNI
Mr. Jeffrey Green	DoD Office of General Counsel
Mr. Steve Homeyer	ODNI
Mr. Mitchell Komaroff	DoD CIO
Mr. James Kren	Defense Security Service
Mr. Jeremy Leader	SAF/AQX
Mr. Richard Naylor	Defense Security Service
Dr. Daniel Radack	Institute for Defense Analyses
Mr. William Stephens	Defense Security Service
Ms. Ann Willis	ODNI

### **May 28–29, 2015**

Mr. Jon Boyens	NIST
Mr. Donald Davidson	DoD CIO
Dr. Lester Foster III	EWA, Inc.
LTC Christian Lewis	DIA
Mr. Emile Monette	GSA
Mr. John Pistolessi	DIA
Ms. Angela Smith	GSA
Mr. Leo Smith	ASA(ALT)
Mr. Randy Trzeciak	CMU SEI
Mr. Thomas Tyndall	DIA
Mr. Elijah Varga	Army PEO for Missiles and Space

### **June 11–12, 2015**

Mr. Brandon Ahrens	Ernst & Young LLP
Mr. Paul Donato	Ernst & Young LLP
Mr. Phillip Harlow	XTAR LLC
Mr. John Hauser	Ernst & Young LLP
Ms. Doree Keating	Ernst & Young LLP
Mr. Alfred Lewis Jr.	Boeing
Mr. Victor Manzueta	Joint Staff (J6)



**Briefers to the Study**

Lt Col John Smail  
Mr. Andras Robert Szakal  
Mr. Vijay Takanti

Joint Staff (J6)  
IBM  
EXOSTAR

**July 30–31, 2015**

Ms. Karen Abell  
Ms. Kristen Baldwin  
Mr. Arthur Beauchamp  
Mr. Ron Fodor  
Mr. Brent Gerity  
Mr. Ted Glum  
Mr. James Gosler  
Ms. Doreen Harwood  
Dr. James Hayward  
Ms. Missy Hebb  
Ms. Janice Meraglia  
Mr. Roy Wilson  
Mr. Raymond Shanahan

U.S. Navy Naval Air Systems Command  
OUSD(AT&L)  
Defense Logistics Agency  
Leidos, Inc.  
Leidos, Inc.  
Defense Microelectronics Activity  
The Johns Hopkins University Applied Physics Laboratory  
Leidos, Inc.  
Applied DNA Sciences  
U.S. Navy Naval Air Systems Command  
Applied DNA Sciences  
U.S. Navy Naval Air Systems Command  
OUSD(AT&L)

**August 13–14, 2015**

Ms. Edna Conway  
Ms. Danielle Curcio  
Mr. Geoff Donatelli  
Ms. Holly Dunlap  
Ms. Ellen Lux  
Mr. Theodore Shpak  
Mr. Michael Smith  
Dr. James Wade

Cisco Systems, Inc.  
Raytheon Company  
Raytheon Company  
Raytheon Company  
Raytheon Company  
Raytheon Company  
Raytheon Company  
Raytheon Company

**September 17–18, 2015**

Mr. Keith Bergevin  
Mr. David Brown  
Dr. Ed Cole  
Mr. John Day  
Mr. George Duchak  
Mr. Alex Gantman  
Mr. Ted Glum  
Mr. Steve McNeil  
Mr. Ron Minnich

Defense Microelectronics Activity  
Intel Corporation  
Sandia National Laboratories  
IBM  
DIUx  
Qualcomm  
Defense Microelectronics Activity  
Xilinx Corporation  
Google



**Briefers to the Study**

Mr. Jason Moore	Xilinx Corporation
Mr. Enrique Oti	DIUx

**October 29–30, 2015**

Dr. Carlos Aquayo-Gonzalez	PFP Cybersecurity
Mr. Thurston Brooks	PFP Cybersecurity
Dr. Boyd Livingston	NSA
Dr. Ian Levy	United Kingdom GCHQ
Mr. Richard Naylor	Defense Security Service
Mr. Stanley Sims	Defense Security Service
Mr. William Stephens	Defense Security Service

**February 4–5, 2016**

Ms. Kristen Baldwin	OUSD(AT&L)
Mr. Kerry Bernstein	DARPA
Mr. Robert Gold	OUSD(AT&L)
Mr. Brian Hughes	OUSD(AT&L)
Ms. Trisha Thibodaux	OUSD(AT&L)
Mr. Christian Thomasson	U.S. Air Force

**April 18–19, 2016**

COL Matthew Dunlop	U.S. Army Cyber Command
Mr. Larry Jennings	ASA(ALT)